x

Summarizing Webroot's Threat Blog Posts for December (2014-01-06 17:07)

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for December, 2013. You can subscribe to [2]**Webroot's Threat Blog RSS Feed**, or follow me on Twitter: **01.** [3]Cybercrime-friendly VPN service provider pitches itself as being 'recommended by Edward Snowden'

02. [4]Commercial Windows-based compromised Web shells management application spotted in the wild **03.** [5]Compromised legitimate Web sites expose users to malicious Java/Symbian/Android “Browser Updates”

04. [6]Malicious multi-hop iframe campaign affects thousands of Web sites, leads to a cocktail of client-side exploits

– part two

05. [7]How cybercriminals efficiently violate YouTube, Facebook, Twitter, Instagram, SoundCloud and Google+’s ToS

06. [8]Tumblr under fire from DIY CAPTCHA-solving, proxies-supporting automatic account registration tools **07.** [9]Newly launched ‘HTTP-based botnet setup as a service’ empowers novice cybercriminals with bulletproof hosting capabilities – part three

5

08. [10]Cybercriminals offer fellow cybercriminals training in Operational Security (OPSEC) **09.** [11]Fake ‘WhatsApp Missed Voicemail’ themed emails lead to pharmaceutical scams **10.** [12]A peek inside the booming underground market for stealth Bitcoin/Litecoin mining tools **11.** [13]Cybercrime Trends 2013 – Year in Review

This post has been reproduced from [14]Dancho Danchev’s blog . Follow him [15]on Twitter.

1. http://www.webroot.com/blog

2. http://feeds2.feedburner.com/WebrootThreatBlog

3. http://www.webroot.com/blog/2013/12/03/cybercrime-friendly-vpn-service-provider-pitches-recommended-edwar

d-snowden/

4. http://www.webroot.com/blog/2013/12/04/commercial-windows-based-compromised-web-shells-management-applica

tion-spotted-wild/

5. http://www.webroot.com/blog/2013/12/05/compromised-legitimate-web-sites-expose-users-malicious-javasymbia

nandroid-browser-updates/

6. http://www.webroot.com/blog/2013/12/09/malicious-multi-hop-iframe-campaign-affects-thousands-web-sites-le

ads-cocktail-client-side-exploits-part-two/

7.

http://www.webroot.com/blog/2013/12/11/cybercriminals-efficiently-violate-monetize-youtube-facebook-twitt

er-instagram-soundcloud-googles-tos/

8. http://www.webroot.com/blog/2013/12/12/tumblr-fire-diy-captcha-solving-proxies-supporting-automatic-accou

nt-registration-tools/

9. http://www.webroot.com/blog/2013/12/16/newly-launched-http-based-botnet-setup-service-empowers-novice-cyb

ercriminals-bulletproof-hosting-capabilities-part-three

10.
http://www.webroot.com/blog/2013/12/17/cybercriminals-offer-fellow-cybercriminals-training-in-operational

-security-opsec/

11. http://www.webroot.com/blog/2013/12/17/cybercriminals-offer-fellow-cybercriminals-training-in-operational

-security-opsec/

12. http://www.webroot.com/blog/2013/12/19/peek-inside-booming-underground-market-stealth-bitcoin-litecoin-mi

ning-tools/

13. http://www.webroot.com/blog/2013/12/27/cybercrime-trends-2013-year-review/

14. http://ddanchev.blogspot.com/

15. http://twitter.com/danchodanchev

Fake Adobe Flash Player Serving Campaign Utilizes Google Hosting/Redirection Infrastructure, Spreads

Across Facebook (2014-01-07 21:09)

What "better" time to spread malicious "joy", then during the Holidays? Cybercriminals are still busy maintaining a fake Adobe Flash Player serving, Facebook spreading campaign, which I originally intercepted during the Holidays, utilizing Google redirectors/hosting services. Despite the modest – naturally conservative estimate – click-through rate (45,000 clicks) compared to that of the most recently profiled similar [1]**Febipos spreading campaign**, which

[2]**resulted in over 1 million clicks**, the campaign remains active, and continues tricking users into installing the rogue Adobe Flash Player, resulting in the continued spread of the campaign, on the Facebook Walls of socially engineered users.

Let’s dissect the campaign, expose its infrastructure/command and control servers, and provide MD5s of the served malware.

Spamvertised

Facebook

URL+redirection

chain:

hxxp://goo.gl/QeshtO;

hxxp://goo.gl/vVbrHp;

hxxp://goo.gl/0oSJ7z; *hxxp://goo.gl/38qIq8*; *hxxp://goo.gl/QNQhc5 -> hxxps://9dvme0lk2r0osqg3qb3rlk95z.storag-e.googleapis.com/q1fwum32gld35 iab9d2u4o35bjsvhjhu309.html?ref=12 ->*

hxxp://goo.gl/wKXme1 -> hxxp://www.i-justice.org/g-o-27312-gooenn.html

(**94.23.166.27**)

->

hxxp://f3c47a0d01f3ec343f57-2ba5bba9317af81ae21c42000295a455.r9.cf4.

-

rackcdn.com/24471bmbqv07595?ref=27312

&aff

_sub=27312

&sub

_id=27312

->

hxxp://www.eklentidunyasi.com/dl.php (**176.31.2.155**) or *hxxp://www.agentofex.com/dl.php* (**176.227.218.99**; www.puee.in) ->

hxxp://docs.google.com/uc?export=download

&id=0B6DFdqpSFDAlSmpsTkZkT2hvN28

or

hxxps://doc-

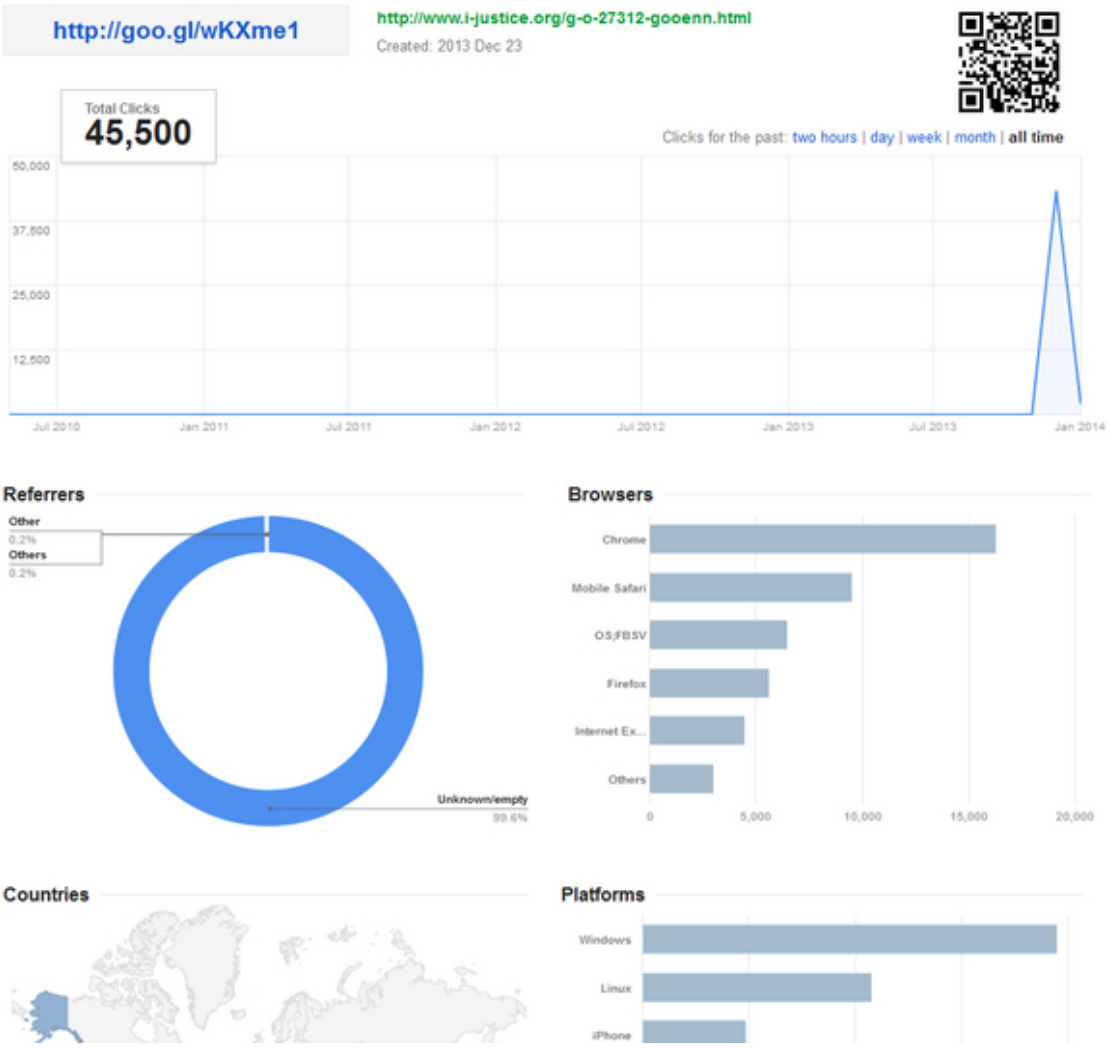
0g-4o-docs.googleusercontent.com/docs/securesc/ha0ro937gcu

c7l7deffksulhg5h7mbp1/7fbm9gn-

67t8t18r8etd00juf0rvmrrmh/1387836000000/16300082901287672546//0BzU3dARQGry0TlMxN3F2STN0Z3M*

GA Account ID: UA-36486228-1

7



Detection rate for the served malware: [3]**MD5: 30118bec581f80de46445aef79e6cf10** - detected by 33 out of 48

antivirus scanners as Trojan-Ransom.Win32.Blocker.dbud.

Once executed, the sample phones back to:

hxxp://176.31.2.155/extFiles/control8.txt

hxxp://176.31.2.155/extFiles/NewFile0008.exe

hxxp://176.31.2.155/extFiles/version.txt

hxxp://176.31.2.155/extFiles/list.txt

hxxp://176.31.2.155/extFiles/list.txt

hxxp://176.31.2.155/extFiles/buflash.xpi

hxxp://176.31.2.155/extFiles/bune10.zip

hxxp://176.31.2.155/extFiles/private/sandbox _status.php

hxxp://176.31.2.155/extFiles/extFiles/yok.txt

The files were offline in time of processing of the sample.

Related MD5s for the same served fake Adobe Flash Player:

MD5: 61f5af5d0067ea8d10f0764ff3c82066

MD5: 80b9ef43183abdd5b22482bc1cea7b36

MD5: 2da7cb838234eebbca3115fcafd6f513

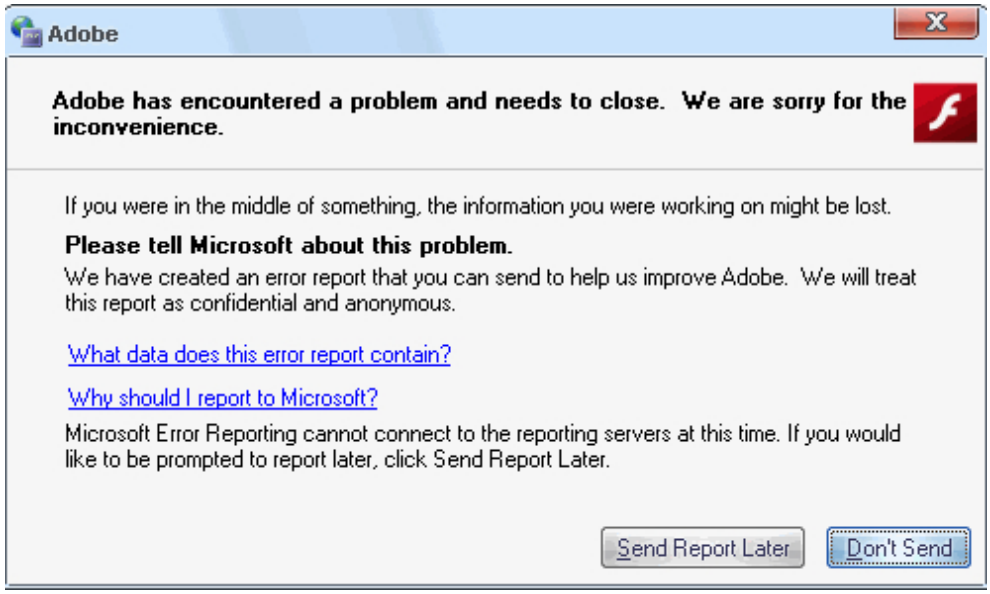
MD5: 40ae8d901102ee3951c241b394eb94e9

MD5: 30118bec581f80de46445aef79e6cf10

MD5: 2de9865032e997d59c03bfd8435f1ada

MD5: fce013bec7b3651c100b6887c0a12eee

9



Once executed, MD5: fce013bec7b3651c100b6887c0a12eee phones back to:

hxxp://176.227.218.99/extFiles/control17.txt

hxxp://176.227.218.99/extFiles/NewFile00017.exe

hxxp://46.163.100.240/NewFile00017.exe

hxxp://176.227.218.99/NewFile00017.exe

hxxp://176.227.218.99/extFiles/extFiles/version.txt

hxxp://176.227.218.99/extFiles/extFiles/list.txt

hxxp://176.227.218.99/extFiles/extFiles/buflash.xpi

hxxp://176.227.218.99/extFiles/extFiles/bune10.zip

Files remain offline in the time of processing of the sample.

This post has been reproduced from [4]Dancho Danchev's blog . Follow him [5]on Twitter.

1. http://ddanchev.blogspot.com/2013/12/continuing-facebook-whos-viewed-your.html

2. http://ddanchev.blogspot.com/2013/12/facebook-circulating-whos-viewed-your.html

3. https://www.virustotal.com/en/file/adec1707efaa1496691d5d4b12daaadff893b0f0ad68b33699e5dd7dd6f8eb58/analysis/1387838333/

4. http://ddanchev.blogspot.com/

5. http://twitter.com/danchodanchev

10

Fake Adobe Flash Player Serving Campaign Utilizes Google Hosting/Redirection Infrastructure, Spreads Across Facebook (2014-01-07 21:09)

What "better" time to spread malicious "joy", then during the Holidays? Cybercriminals are still busy maintaining a fake Adobe Flash Player serving, Facebook spreading campaign, which I originally intercepted during the Holidays, utilizing Google redirectors/hosting services. Despite the modest – naturally conservative estimate – click-through rate (45,000 clicks) compared to that of the most recently profiled similar [1]**Febipos spreading campaign**, which

[2]**resulted in over 1 million clicks**, the campaign remains active, and continues tricking users into installing the rogue Adobe Flash Player, resulting in the continued spread of the campaign, on the Facebook Walls of socially engineered users.

Let’s dissect the campaign, expose its infrastructure/command and control servers, and provide MD5s of the served malware.

Spamvertised

Facebook

URL+redirection

chain:

hxxp://goo.gl/QeshtO;

hxxp://goo.gl/vVbrHp;

hxxp://goo.gl/0oSJ7z; *hxxp://goo.gl/38qIq8*; *hxxp://goo.gl/QNQhc5 -> hxxps://9dvme0lk2r0osqg3qb3rlk95z.storag-*

e.googleapis.com/q1fwum32gld35 iab9d2u4o35bjsvhjhu309.html?ref=12 -> hxxp://goo.gl/wKXme1 -> hxxp://www.i-justice.org/g-o-27312-gooenn.html

(**94.23.166.27**)

->

hxxp://f3c47a0d01f3ec343f57-2ba5bba9317af81ae21c42000295a455.r9.cf4.

-

rackcdn.com/24471bmbqv07595?ref=27312

&aff

_sub=27312

&sub

_id=27312

->

hxxp://www.eklentidunyasi.com/dl.php (**176.31.2.155**) or *hxxp://www.agentofex.com/dl.php* (**176.227.218.99**; www.puee.in) ->

hxxp://docs.google.com/uc?export=download

&id=0B6DFdqpSFDAlSmpsTkZkT2hvN28

or

hxxps://doc-

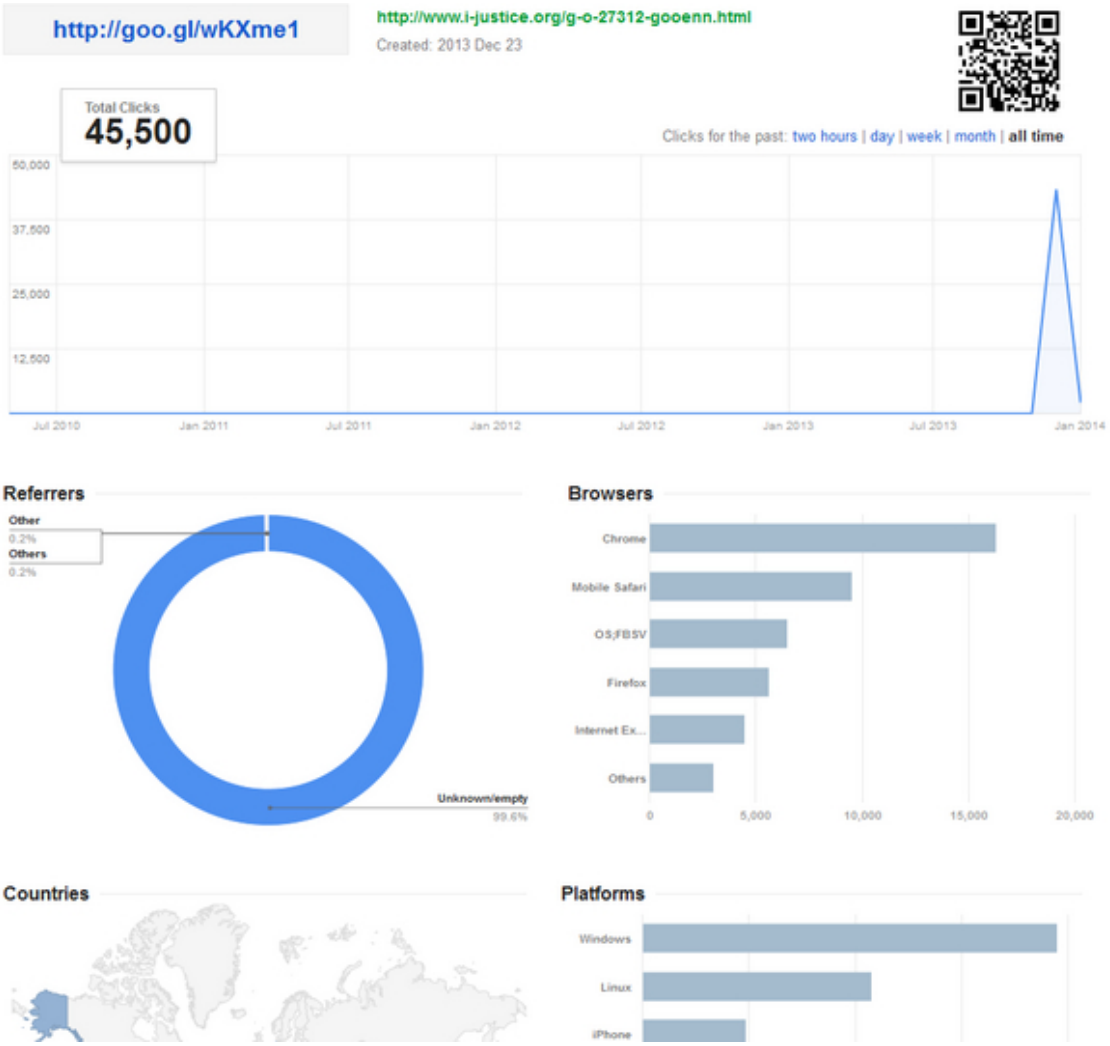
0g-4o-docs.googleusercontent.com/docs/securesc/ha0ro937gcu

c7l7deffksulhg5h7mbp1/7fbm9gn-

67t8t18r8etd00juf0rvmrrmh/1387836000000/16300082901287672546//0BzU3dARQGry0TlMxN3F2STN0Z3M*

GA Account ID: UA-36486228-1

11



Detection rate for the served malware: [3]**MD5: 30118bec581f80de46445aef79e6cf10** - detected by 33 out of 48

antivirus scanners as Trojan-Ransom.Win32.Blocker.dbud.

Once executed, the sample phones back to:

hxxp://176.31.2.155/extFiles/control8.txt

hxxp://176.31.2.155/extFiles/NewFile0008.exe

hxxp://176.31.2.155/extFiles/version.txt

hxxp://176.31.2.155/extFiles/list.txt

hxxp://176.31.2.155/extFiles/list.txt

hxxp://176.31.2.155/extFiles/buflash.xpi

hxxp://176.31.2.155/extFiles/bune10.zip

hxxp://176.31.2.155/extFiles/private/sandbox _status.php

hxxp://176.31.2.155/extFiles/extFiles/yok.txt

The files were offline in time of processing of the sample.

Related MD5s for the same served fake Adobe Flash Player:

MD5: 61f5af5d0067ea8d10f0764ff3c82066

MD5: 80b9ef43183abdd5b22482bc1cea7b36

MD5: 2da7cb838234eebbca3115fcafd6f513

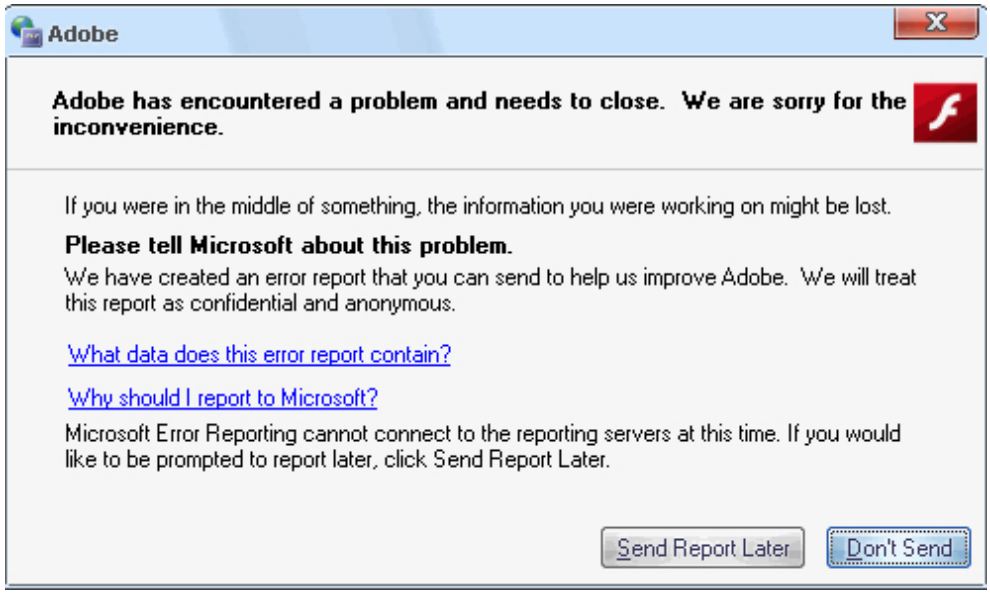
MD5: 40ae8d901102ee3951c241b394eb94e9

MD5: 30118bec581f80de46445aef79e6cf10

MD5: 2de9865032e997d59c03bfd8435f1ada

MD5: fce013bec7b3651c100b6887c0a12eee

13



Once executed, MD5: fce013bec7b3651c100b6887c0a12eee phones back to:

hxxp://176.227.218.99/extFiles/control17.txt

hxxp://176.227.218.99/extFiles/NewFile00017.exe

hxxp://46.163.100.240/NewFile00017.exe

hxxp://176.227.218.99/NewFile00017.exe

hxxp://176.227.218.99/extFiles/extFiles/version.txt

hxxp://176.227.218.99/extFiles/extFiles/list.txt

hxxp://176.227.218.99/extFiles/extFiles/buflash.xpi

hxxp://176.227.218.99/extFiles/extFiles/bune10.zip

Files remain offline in the time of processing of the sample.

1. http://ddanchev.blogspot.com/2013/12/continuing-facebook-whos-viewed-your.html

2. http://ddanchev.blogspot.com/2013/12/facebook-circulating-whos-viewed-your.html

3. https://www.virustotal.com/en/file/adec1707efaa1496691d5d4b12daaadff893b0f0ad68b33699e5dd7dd6f8eb58/analysis/1387838333/

Dissecting the Ongoing Febipos/Carfekab Rogue Chrome/Firefox Extensions Dropping, Facebook Circulating Malicious Campaign (2014-01-09 17:21)

And, (not surprisingly) they're back! The cybercriminal(s) behind the 1 million+ clicks strong Febipos/Carfekab rogue Chrome/Firefox extensions dropping malicious campaign, continue utilizing the already infected 'population' for the purpose of disseminating the newly packed/modified extensions/samples across Facebook, with yet another campaign that I'll dissect in this post.

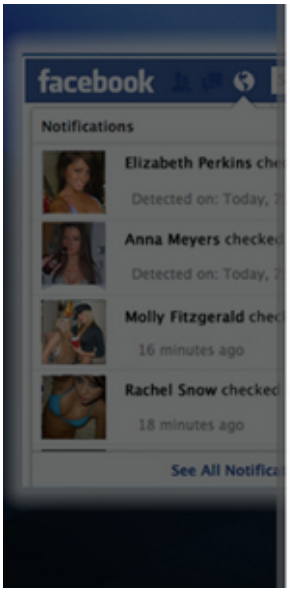
Catch up with previous research dissecting the previous campaigns:

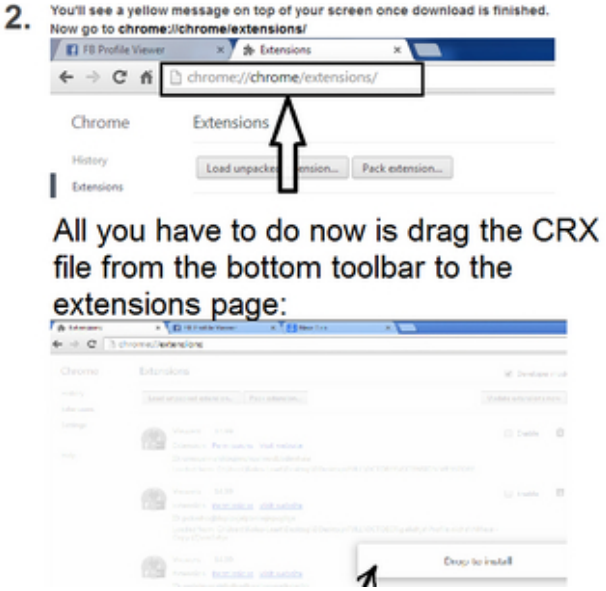
• [1]Facebook Circulating 'Who's Viewed Your Profile' Campaign Exposes 800k+ Users to CrossRider PUA/Rogue Firefox Add-ons/Android Adware AirPush

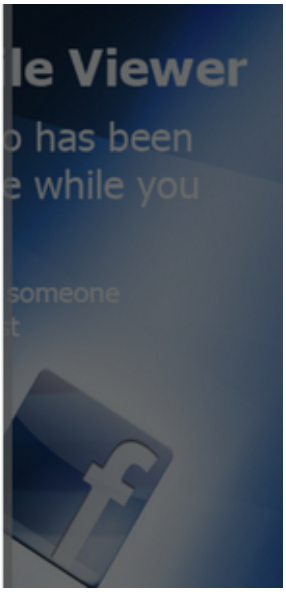
• [2]Continuing Facebook "Who's Viewed Your Profile" Campaign Affects Another 190k+ Users, Exposes Malicious Cybercrime Ecosystem

Redirection chain: *hxxp://GXOMZRC.tk/?74604844* (**93.170.52.34**) -> *hxxp://wqeuijlks.igg.biz/?asdjas22222222-222222* (**88.198.132.3**) ->

hxxp://prostats.vf1.us/s.htm -> hxxp://vidsvines.com/d/ -> hxxp://vidsvines.com/d/firefox 15







->

hxxp://vidsvines.com/d/ch/ -> hxxp://vidsvines.com/d/ch/profile2.html (**192.157.201.42**)
First GA Account ID: UA-23441223-3

Second GA Account ID: UA-25941572-1

Actual malicious content hosting locations (legitimate infrastructure again):
hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqVFgyZzFzR1o3YTQ &export=download
hxxps://dl.dropboxusercontent.com/s/tj9n05qhjvnkg4s/whoviewsfam.xp i

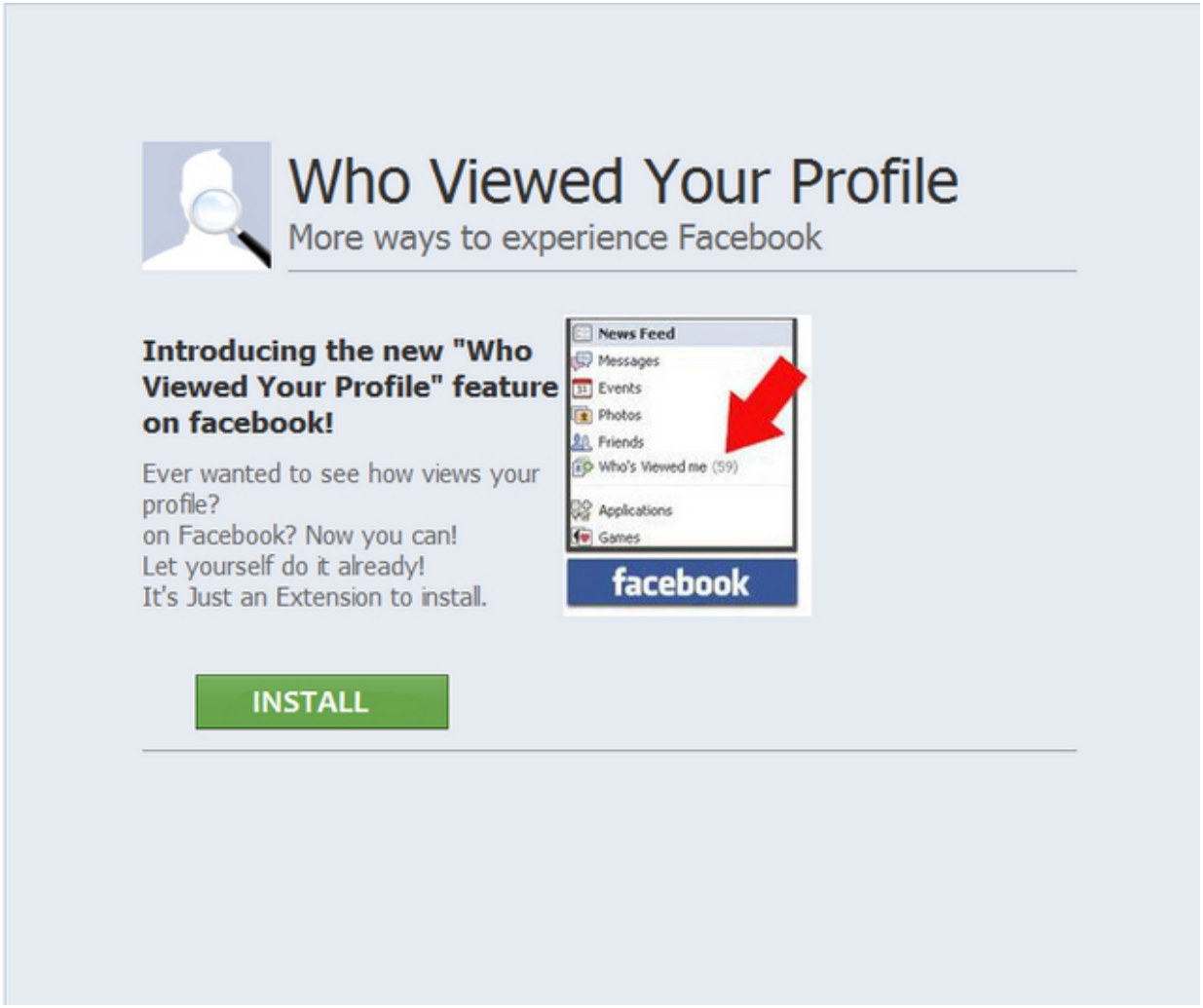
Detection rates for the served rogue Chrome/Firefox extensions:

[3]**MD5: 0ee44443c73bd9b072c7f1dbb6b7b591**

[4]**MD5: c4953f63ab46c796e23388f9c1cfa273**

[5]**MD5: 5bcec283594e863f5dd238e2d22446c7**

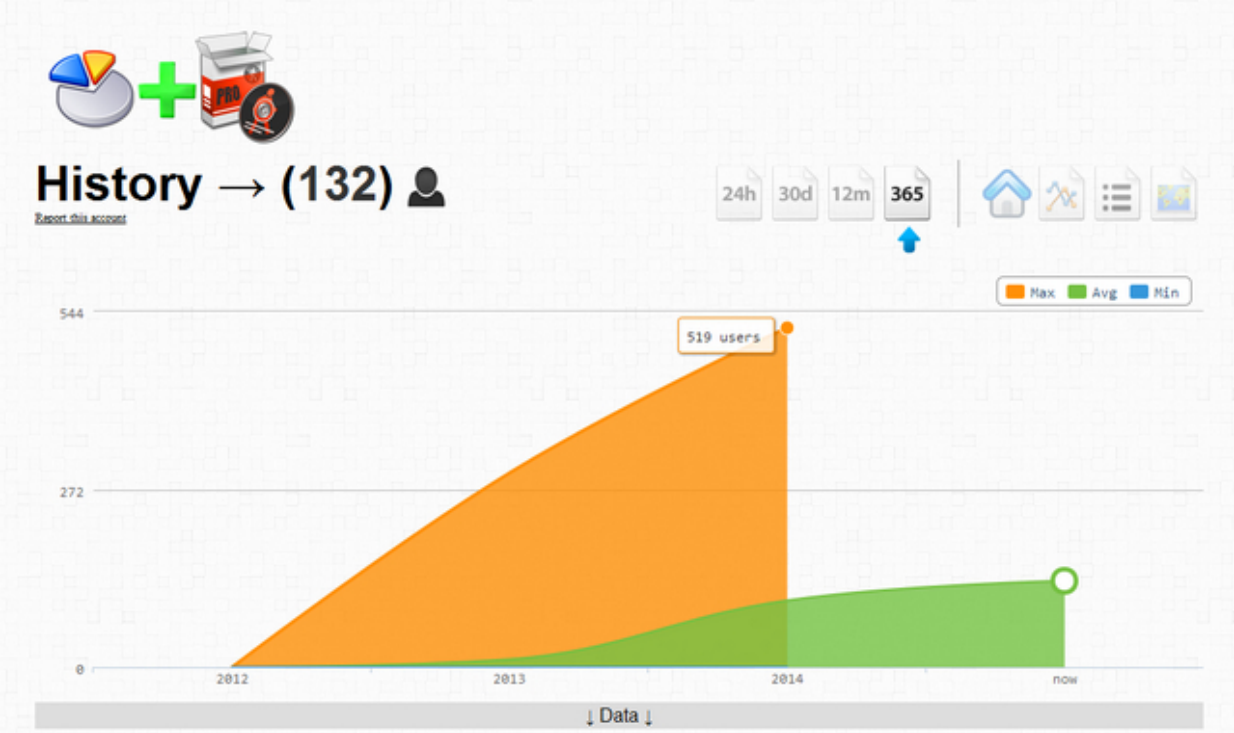
16



Once executed, [6]**MD5: 5bcec283594e863f5dd238e2d22446c7** drops **MD5: deb483270b9ed5da7fcf1d01a6fde8a7**

and **MD5: 90b77a477d815c771559d08ea80cc0c8** it then phones back to 212.117.32.20.

17



Related malicious MD5s known to have phoned back to the same IP:

MD5: 33408f35623dc5bb4a3bde09fa45f86b

MD5: 56a54a700ae5700c3cd3da9c2ad226cf

MD5: f868123050391 56b1da8fc29bdddebb7

MD5: ede8f20d78a81c7da76ad7def37ebbdd

This post has been reproduced from [7]Dancho Danchev's blog . Follow him [8]on Twitter.

1. http://ddanchev.blogspot.com/2013/12/facebook-circulating-whos-viewed-your.html

2. http://ddanchev.blogspot.com/2013/12/facebook-circulating-whos-viewed-your.html

3. https://www.virustotal.com/en/file/ae0ac523f752b320a103befeacfc960e6f86b01343d7598f48664afcb4cedd71/analysis/1389277417/

4. https://www.virustotal.com/en/file/dd46cd6ec5b139f55a9ddec75fed261568c06abf1883cf28dc1f5a3491c3e0c1/analysis/1389277591/

5. https://www.virustotal.com/en/file/7737cf0c74e5e84f543a379ff9e42ac372f78ff0e8eb4c847a7bc4d07f8b1368/analysis/1389277807/

6. https://www.virustotal.com/en/file/7737cf0c74e5e84f543a379ff9e42ac372f78ff0e8eb4c847a7bc4d07f8b1368/analysis/1389277807/

7. http://ddanchev.blogspot.com/

8. http://twitter.com/danchodanchev

Dissecting the Ongoing Febipos/Carfekab Rogue Chrome/Firefox Extensions Dropping, Facebook Circulating Malicious Campaign (2014-01-09 17:21)

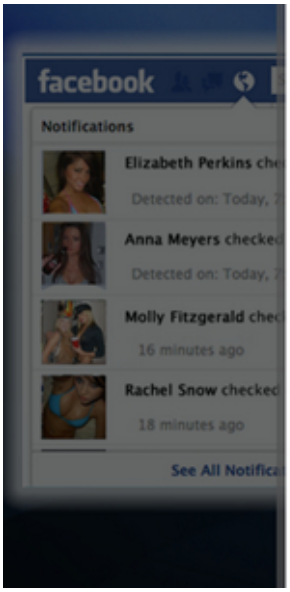
And, (not surprisingly) they're back! The cybercriminal(s) behind the 1 million+ clicks strong Febipos/Carfekab rogue Chrome/Firefox extensions dropping malicious campaign, continue utilizing the already infected 'population' for the purpose of disseminating the newly packed/modified extensions/samples across Facebook, with yet another campaign that I'll dissect in this post.

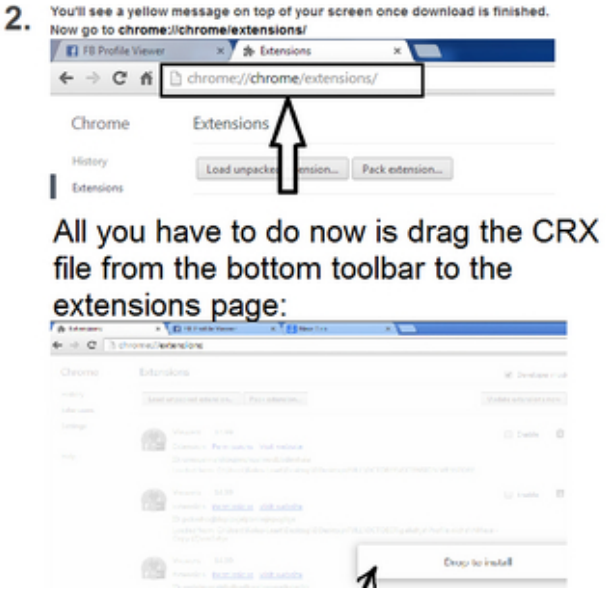
Catch up with previous research dissecting the previous campaigns:

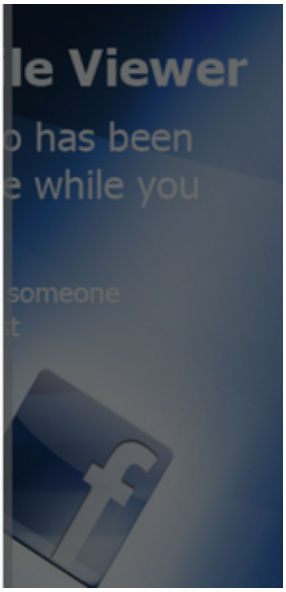
• [1]Facebook Circulating ’Who’s Viewed Your Profile’ Campaign Exposes 800k+ Users to CrossRider PUA/Rogue Firefox Add-ons/Android Adware AirPush

• [2]Continuing Facebook "Who’s Viewed Your Profile" Campaign Affects Another 190k+ Users, Exposes Malicious Cybercrime Ecosystem

Redirection chain: *hxxp://GXOMZRC.tk/?74604844* (**93.170.52.34**) -> *hxxp://wqeuijlks.igg.biz/?asdjas22222222-222222* (**88.198.132.3**) -> *hxxp://prostats.vf1.us/s.htm -> hxxp://vidsvines.com/d/ -> hxxp://vidsvines.com/d/firefox* 19







->

hxxp://vidsvines.com/d/ch/ -> hxxp://vidsvines.com/d/ch/profile2.html (**192.157.201.42**)
First GA Account ID: UA-23441223-3

Second GA Account ID: UA-25941572-1

Actual malicious content hosting locations (legitimate infrastructure again):
hxxps://docs.google.com/uc?authuser=0 &id=0BziH-mKCuQwqVFgyZzFzR1o3YTQ &export=download
hxxps://dl.dropboxusercontent.com/s/tj9n05qhjvnkg4s/whoviewsfam.xp i

Detection rates for the served rogue Chrome/Firefox extensions:

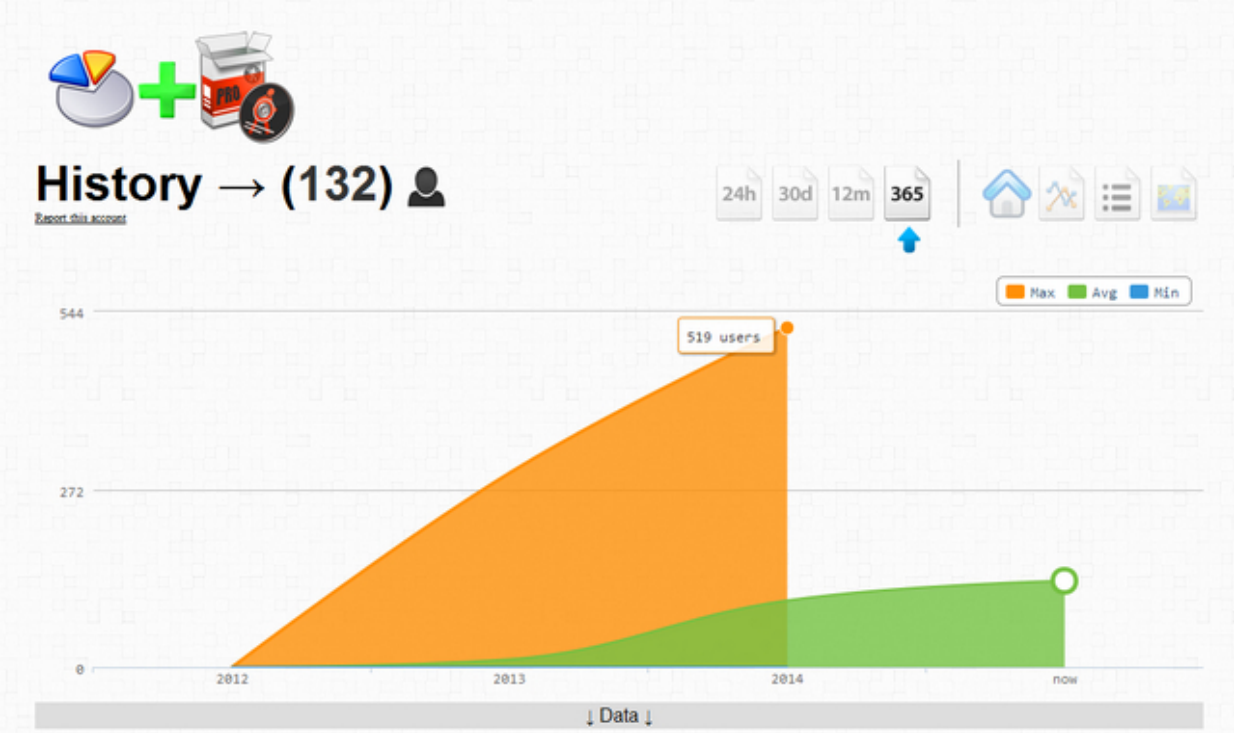
[3]**MD5: 0ee44443c73bd9b072c7f1dbb6b7b591**

[4]**MD5: c4953f63ab46c796e23388f9c1cfa273**

[5]**MD5: 5bcec283594e863f5dd238e2d22446c7**

Once executed, [6]**MD5: 5bcec283594e863f5dd238e2d22446c7** drops **MD5: deb483270b9ed5da7fcf1d01a6fde8a7**

and **MD5: 90b77a477d815c771559d08ea80cc0c8** it then phones back to 212.117.32.20.



Related malicious MD5s known to have phoned back to the same IP:

MD5: 33408f35623dc5bb4a3bde09fa45f86b

MD5: 56a54a700ae5700c3cd3da9c2ad226cf

MD5: f868123050391 56b1da8fc29bdddebb7

MD5: ede8f20d78a81c7da76ad7def37ebbdd

Updates will be posted as soon as new developments take place.

1. http://ddanchev.blogspot.com/2013/12/facebook-circulating-whos-viewed-your.html

2. http://ddanchev.blogspot.com/2013/12/facebook-circulating-whos-viewed-your.html

3.
https://www.virustotal.com/en/file/ae0ac523f752b320a103befeacfc960e6f86b01343d7598f48664afcb4cedd71/analysis/1389277417/

4.
https://www.virustotal.com/en/file/dd46cd6ec5b139f55a9ddec75fed261568c06abf1883cf28dc1f5a3491c3e0c1/analysis/1389277591/

5.
https://www.virustotal.com/en/file/7737cf0c74e5e84f543a379ff9e42ac372f78ff0e8eb4c847a7bc4d07f8b1368/analysis/1389277807/

6.
https://www.virustotal.com/en/file/7737cf0c74e5e84f543a379ff9e42ac372f78ff0e8eb4c847a7bc4d07f8b1368/analysis/1389277807/

22

Facebook Spreading,

Amazon AWS/Cloudflare/Google Docs Hosted Campaign,

Serves P2P-

Worm.Win32.Palevo (2014-01-16 21:27)

A currently circulating across Facebook, multi-layered monetization tactics utilizing, Turkish users targeting, malicious campaign, is attempting to trick users into thinking that they need to install a fake Adobe Flash Player, displayed on a fake YouTube Video page, ultimately serving P2P-Worm.Win32.Palevo on the hosts of the socially engineered (international) users.

Let’s dissect the campaign, expose its infrastructure in terms of shortened URLs, redirectors, affiliate network IDs, landing pages, pseudo-random Facebook content generation phone back URLs, legitimate infrastructure hosted content, and provide MD5s for the served malicious content.

Sample

redirection

chain:

hxxp://m3mi.com/10469

->

hxxp://facebookikiziniz.com/yon.html?MYt-

DmZp4xjbUP9A0OHLj

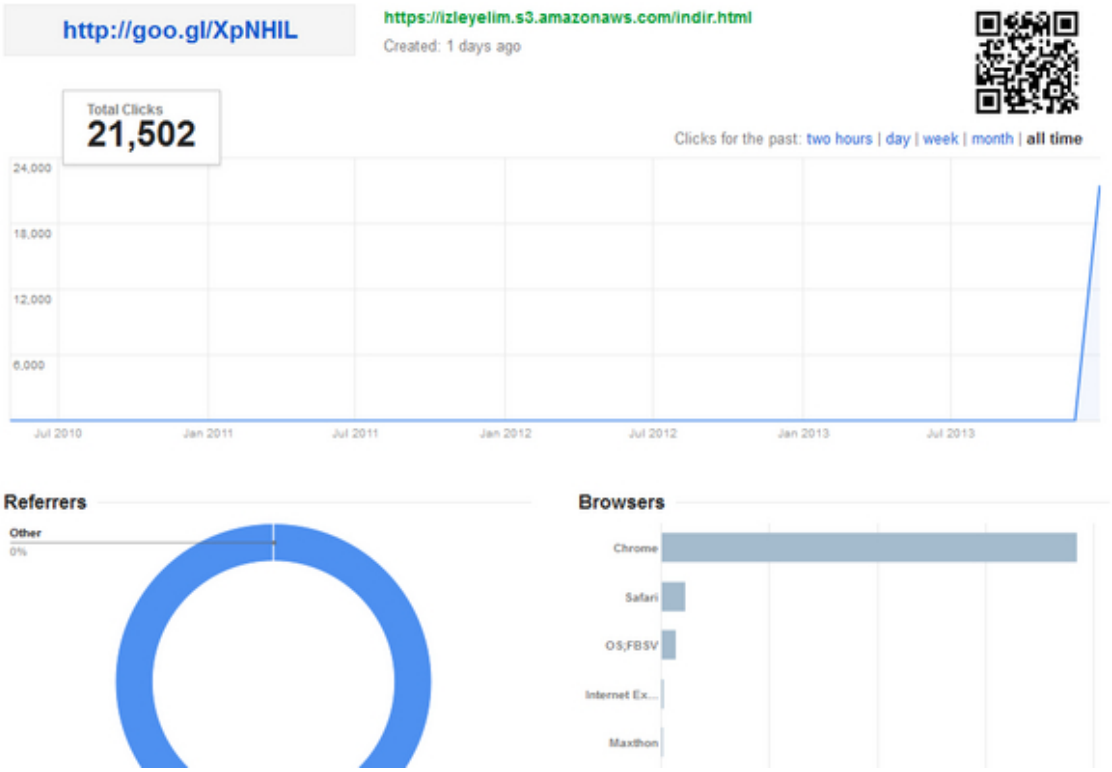
->

hxxp://facebookikiziniz.com/yon.html?
MYtDmZp4xjbUP9A0OHLj

->

hxxp://facebookikiziniz.com/yon.html?
MYtDmZp4xjbUP9A0OHLj

23



Internal campaign redirection structure+associated affiliate network IDs+landing URLs:
hxxp://mobiltrafik.s3.amazonaws.com/mobil.html

hxxp://mobiltrafik.s3.amazonaws.com/yurtdisi-anroid.html ->
hxxp://ad.adrttt.com/aff _c?offer _id=1743 &aff _id=3236
&source=yurtdisi ->
hxxp://ads.glispa.com/sw/49399/CD353/102
3a788c68361b710b87b8ed4851a ->

hxxps://play.google.com/store/apps/details?
id=com.mobogenie.marketstl

hxxp://mobiltrafik.s3.amazonaws.com/yurtdisi-ios.html

->

hxxp://ad.rdrttt.com/aff

_c?offer

_id=302

&aff

_id=1014

->

hxxp://www.freehardcorepassport.com/?t=116216,1,96,0

&x=pornfr

_tracker=9208KOm00B0193IbJl3yk01BNW00005m

hxxp://mobiltrafik.s3.amazonaws.com/yurtdisiweb.html ->
hxxp://ad.rdrttt.com/aff _c?offer _id=302 &aff _id=1014

-> hxxp://ads.polluxnetwork.com/hosted/w2m.php?
tid=1023e4f08cae470c2f74aa 3d1e2d17 &oid=6200
&aid=758

-> hxxp://m.pornfr.3013.idhad.com/xtrem/index.wiml

hxxp://mobiltrafik.s3.amazonaws.com/androidwifi.html ->
hxxp://ad.adrttt.com/aff _c?offer _id=1743 &aff _id=3236

&source=yurtici ->
hxxp://ads.glispa.com/sw/49399/CD353/102

3a788c68361b710b87b8ed4851a
hxxp://mobiltrafik.s3.amazonaws.com/iphonewifi.html ->
hxxp://ad.adrttt.com/aff _c?offer _id=1705 &aff _id=3236

-> hxxps://itunes.apple.com/tr/app/id451786983?mt=8

hxxp://mobiltrafik.s3.amazonaws.com/turkcell.html ->
hxxp://goo.gl/GBKArV

hxxp://mobiltrafik.s3.amazonaws.com/vodofone.html ->
hxxp://ad.adrttt.com/aff _c?offer _id=1785 &aff _id=3236

-> hxxp://c.mobpartner.mobi/?s=1007465 &a=3578
&tid1=102afc4360ecadbed491b5c08f7395

hxxp://mobiltrafik.s3.amazonaws.com/avea.html ->
hxxp://ad.juksr.com/aff _c?offer _id=709 &aff _id=3236

->

hxxp://wap.chatwalk.com/landings/?name=yilbasi2

&affid=reklamaction

&utm

_campaign=3236

&clk=1025fa187aca81ce57edf8adca7a9c

hxxp://mobiltrafik.s3.amazonaws.com/trweb.html ->
hxxp://ad.adrttt.com/aff _c?offer _id=1689 &aff _id=3236

&source=yurticidefault ->
hxxps://www.matchandtalk.com/splashmobile/10?sid=12
&bid=663

hxxp://s3.amazonaws.com/Yonver/tarayici.html ->
hxxp://ad.adrttt.com/aff _c?offer _id=1091 &aff _id=3236

&source=tarayicidan ->
hxxps://www.matchandtalk.com/splash/12?s id=12
&bid=651 &cid=29

hxxp://izleyelim.s3.amazonaws.com/unlu.html

->

hxxp://goo.gl/XpNHIL

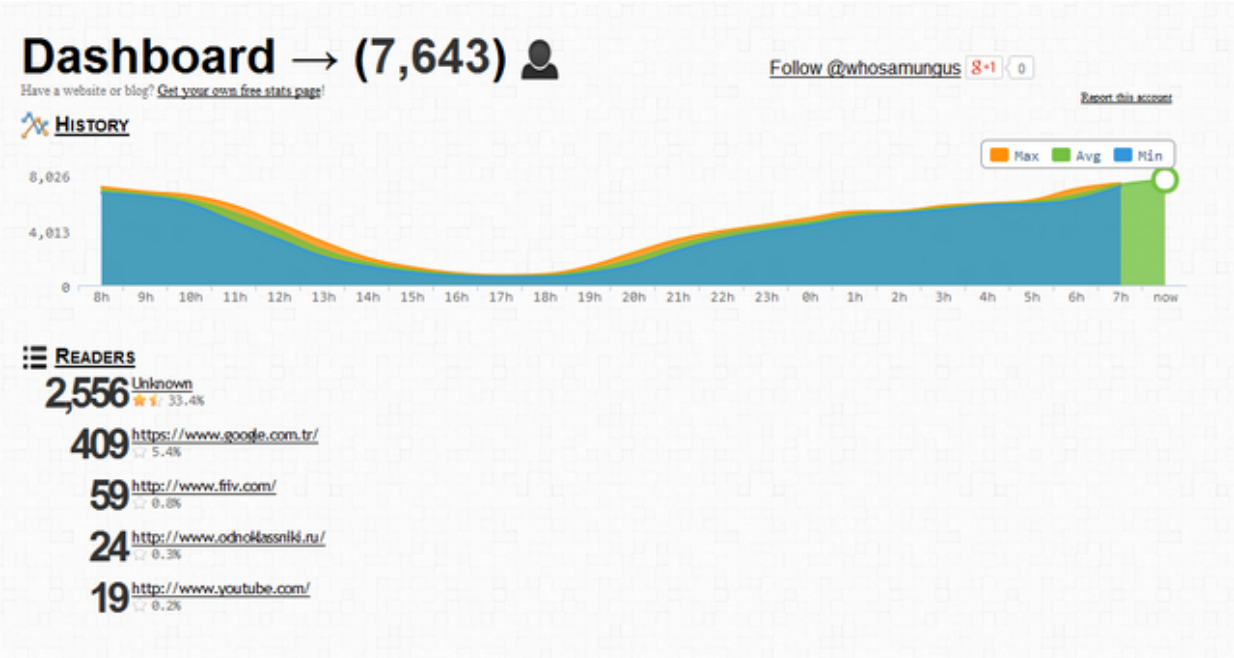
(21,512

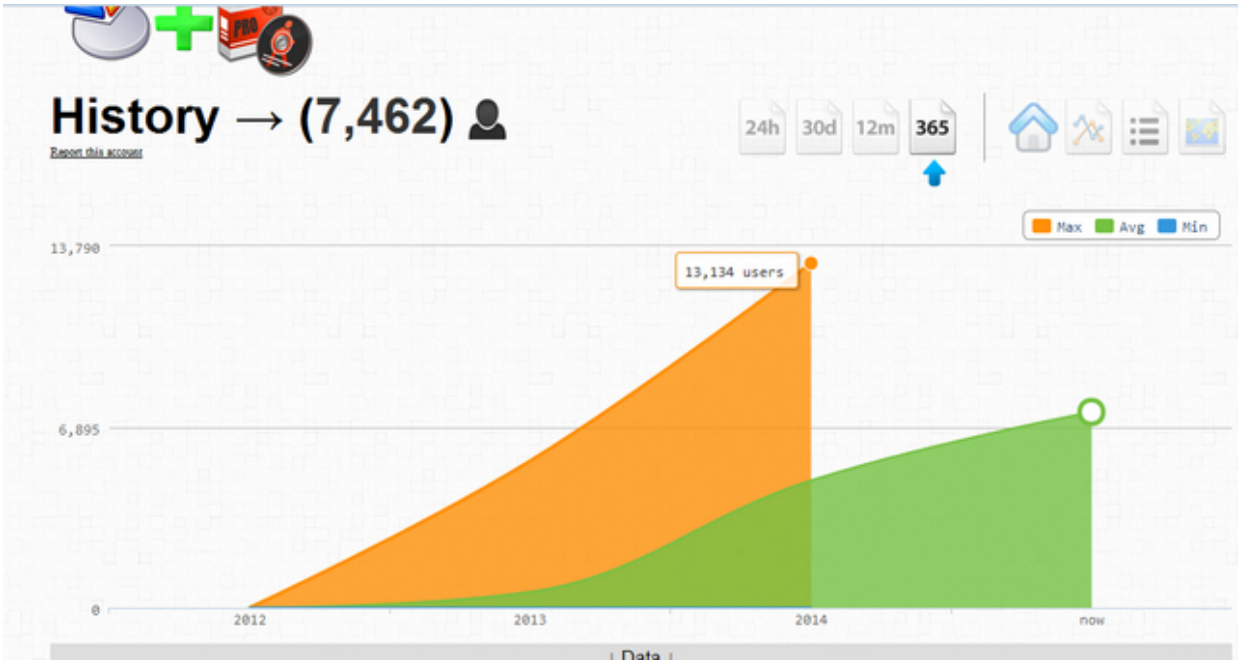
clicks)

->

hxxps://izleyelim.s3.amazonaws.com/indir.html

24





hxxps://s3.amazonaws.com/facebookAds/ortaryon.html

->

hxxps://www.matchandtalk.com/splash/12?sid=12

&bid=651 &cid=29

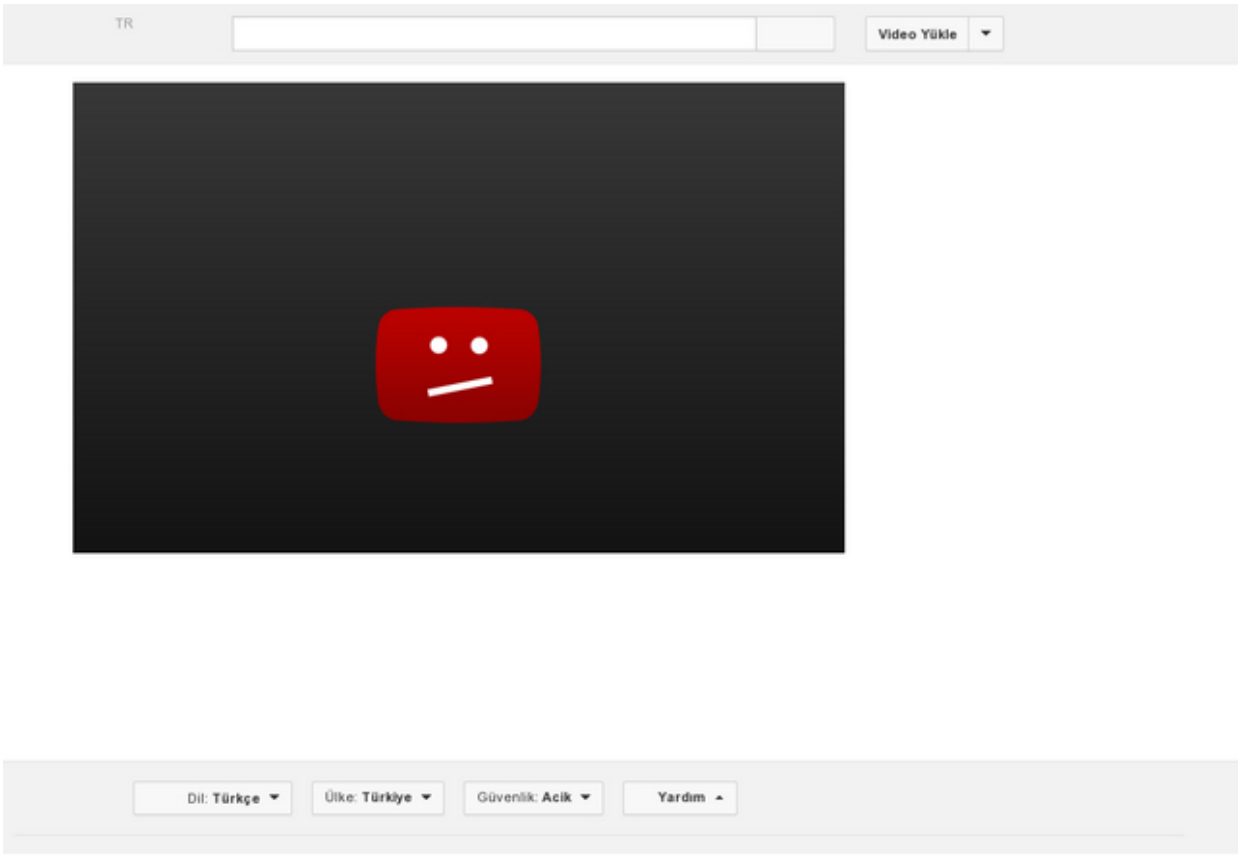
Malicious/fraudulent domain name reconnaissance:

facebookikiziniz.com - 108.162.195.103; 108.162.194.103

ttcomcdn.com - 162.159.241.195; 162.159.242.195 - Email: masallahkilic@hotmail.com amentosx.com - 141.101.116.113; 141.101.117.113

ad.adrttt.com - 54.236.194.194

25



The campaign is also mobile device/PC-aware, and is therefore automatically redirecting users to a variety of different locations/affiliate networks. Case in point, the redirection to Google Play's Mobogenie Market App (Windows application detected as Adware.NextLive.2 [1]**MD5: 9dd785436752a6126025b549be644e76**), and the iOS compatible SK

planet's TicToc app.

Now comes the malicious twist, in the form of Fake Adobe Flash Player, that socially engineered users would have to install, in order to view the non-existent YouTube video content.

Actual Fake Adobe Flash Player hosting locations within Google Docs:

hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH _w8BCFcWZlRGY0V1IxNVU

hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH _w8BCFQVBsdVVOekYyNGs hxxps://docs.google.com//uc? authuser=0 &id=0B9oVyH _w8BCFaEN2TnE4M0sxWHM

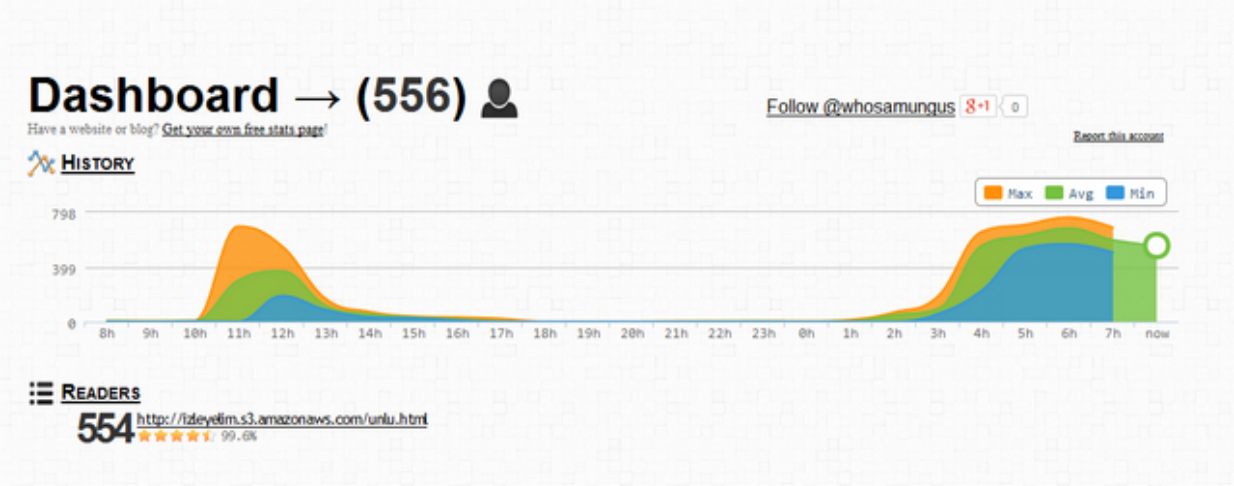
hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH _w8BCFVXRnbkYtNG5wVDA hxxps://docs.google.com//uc? authuser=0 &id=0B9oVyH _w8BCFR2NnRXFRUmtNTTQ

hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH _w8BCFOWFGZnlxMkZWcUE

hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH _w8BCFcWZZbTljMkJWZ3c hxxps://docs.google.com//uc? authuser=0 &id=0B9oVyH _w8BCFYkpEdXI4ZGVaaUE

hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH _w8BCFMUxzY0dQTTJMV00

hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH _w8BCFNmROSXhMSGdCYUU



hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH_w8BCFb0RoZVltMmsyRFU

hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH_w8BCFb2k2MFN4QTY1ZUE

hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH_w8BCFb1AzZXI4emlGR00

hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH_w8BCFSDZBRDJ4QjVqdkU

hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH_w8BCFUXgtZ1VQVU9OdVU

hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH_w8BCFUll6c0Y0MWxLZW8

hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH_w8BCFSW55S3R0SWcxdDQ

hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH_w8BCFMWtxaGJTMnpMVDA hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH _w8BCFSk9yUW5ldDVKaUU

hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH _w8BCFN3pTXzcxcDlObkU

hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH _w8BCFQ0p3dV9qcC1uOFU

hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH _w8BCFOFZRcDZwa0ZfcVk hxxps://docs.google.com//uc? authuser=0 &id=0B9oVyH _w8BCFNkoyNktzQ2dJVlE

hxxps://docs.google.com//uc?authuser=0 &id=0B9oVyH _w8BCFS2xJdTE4Nk04QnM

Detection rate for the fake Adobe Flash Player:

[2]**MD5:**

5bf26bd488503a4b2b74c7393d4136e3 - detected by 3 out of 47 antivirus scanners as P2P-Worm.Win32.Palevo.hexb; PE:Trojan.VBInject!1.6546

Once executed, the sample also drops:

[3]**MD5: a8234e13f9e3af4c768de6f2d6204b3c**

Once executed, the sample phones back to: akillitelefonburada.com (108.162.196.162).

Sample

pseudo-random

bogus

Facebook

content

generation

takes

place

through:

hxxp://www.amentosx.com/ext/r.php

->

hxxps://s3.amazonaws.com/facebookAds/arkadaj.html

->

hxxp://ttcomcdn.com/tw.php

This post has been reproduced from [4]Dancho Danchev's blog . Follow him [5]on Twitter.

1. https://www.virustotal.com/en/file/bc9c9cb2a1219b87cdb9e356b72f2e64c1ac2e9250302e72b426ad51dcc6818f/analysis/1389893847/

2. https://www.virustotal.com/en/file/9c92331776087bc46053dcf388394acdb6faace813153f6f1cd9a9be1ffad0c5/analysis/

3. https://www.virustotal.com/en/file/d792c1ee1f944940f1fabda43392231021596dd546a40eeb0ca407535fbc7820/analysis/

4. http://ddanchev.blogspot.com/

5. http://twitter.com/danchodanchev

28

Şuan sitedeki **985 kişi** toplam **3,457 video**'nun keyfini çıkarıyor.. Sizde onlardan birisi olun!

- kayıt ol
- giriş yap

- anasayfa
- kategoriler
- kanallar

 # Recep İvedik 4 (Full İzle - HD Ücretsiz)

Please install Flash Player...
1 gün önce eklendi
15,547 **kez izlendi**
Paylaş:
Video
© 2011 - unluvideolari.info

- Hızlı Menü
- . anasayfa
- . hakkımızda
- . kategoriler
- . kanallar
- . sss
- . iletişim

- Sosyal Ağlar
- Facebook Sayfamız
- Twitter'dan Takip Edin!
- Videolara Abone Olun!
- İletişime Geçin!

Facebook Spreading,

Amazon AWS/Cloudflare/Google Docs Hosted Campaign,

Serves P2P-

Worm.Win32.Palevo (2014-01-16 21:27)

I’ve recently spotted a malicious, cybercrime-friendly SWF iframe/redirector injecting service, that also exposes a long-run Win32.Nixofro serving malicious infrastructure, currently utilized for the purpose of operating a rogue social media service provider, that’s targeting Turkish Facebook users through the ubiquitous social engineering vector, for such type of campaigns, namely, the fake Adobe Flash player.

Let’s profile the service, discuss its relevance in the broader context of the threat landscape, provide action-able/historical threat intelligene on the malicious infrastructure, the rogue domains involved in it, the malicious MD5s served by the cybercriminals behind it, and directly link it to a [1]**previously profiled Facebook spreading P2P-Worm.Win32.Palevo serving campaign**.

The managed SWF iframe/redirector service, is a great example of a cybercrime-as-a-service type of underground market proposition, empowering, both, sophisticated and novice cybercriminals with the necessary ([2]**malvertising**)

’know-how’, in an efficient manner, directly intersecting with the commercial availability of [3]**sophisticated mass Web site**/[4]**Web server** malicious script embedding platforms.

The managed SWF iframe/redirector injecting service is currently responding to 108.162.197.62 and 108.162.196.62

[redacted]	Обычный	Оптовый	VIP персона
Неделя (7 дней)	5	1	0.5
Месяц (30 дней)	10	2	1
Год (365 дней)	15	5	2

Known to have responded to the same IPs (108.162.197.62; 108.162.196.62) is also a key part of the malicious

infrastructure that I’ll expose in this post, namely **hizliservis.pw** - Email: furkan@cod.com.

Known to have phoned back to the same IP (108.162.197.62) are also the following malicious MD5s: MD5: 432efe0fa88d2a9e191cb95fa88e7b36

MD5: 720ecb1cf4f28663f4ab25eedf620341

MD5: 02691863e9dfb9e69b68f5fca932e729

MD5: 69ed70a82cb35a454c60c501025415aa

MD5: cc586a176668ceef14891b15e1b412ab

MD5: 74291941bddcec131c8c6d531fcb1886

MD5: 7c27d9ff25fc40119480e4fe2c7ca987

MD5: 72c030db7163a7a7bf2871a449d4ea3c

MD5: 432efe0fa88d2a9e191cb95fa88e7b36

Known to have phoned to the same IP (108.162.196.62) are also the following malicious MD5s: MD5: eda3f015204e9565c779e0725915864f

MD5: effcfe91beaf7a3ed2f4ac79525c5fc5

MD5: 14acd831691173ced830f4b51a93e1ca

MD5: 7f93b0c611f7020d28f7a545847b51e0

MD5: bcfce3a9bf2c87dab806623154d49f10

MD5: 4c90a89396d4109d8e4e2491c5da4846

MD5: 289c4f925fdec861c7f765a65b7270af

Sample redirection chain leading to the fake Adobe Flash Player:

hxxp://hizliservis.pw/unlu.htm

->

hxxp://hizliservis.pw/indir.php

->

hxxp://unluvideolari.info

->

hxxp://videotr.in/player.swf

->

hxxp://izleyelim.s3.amazonaws.com/movie.mp4

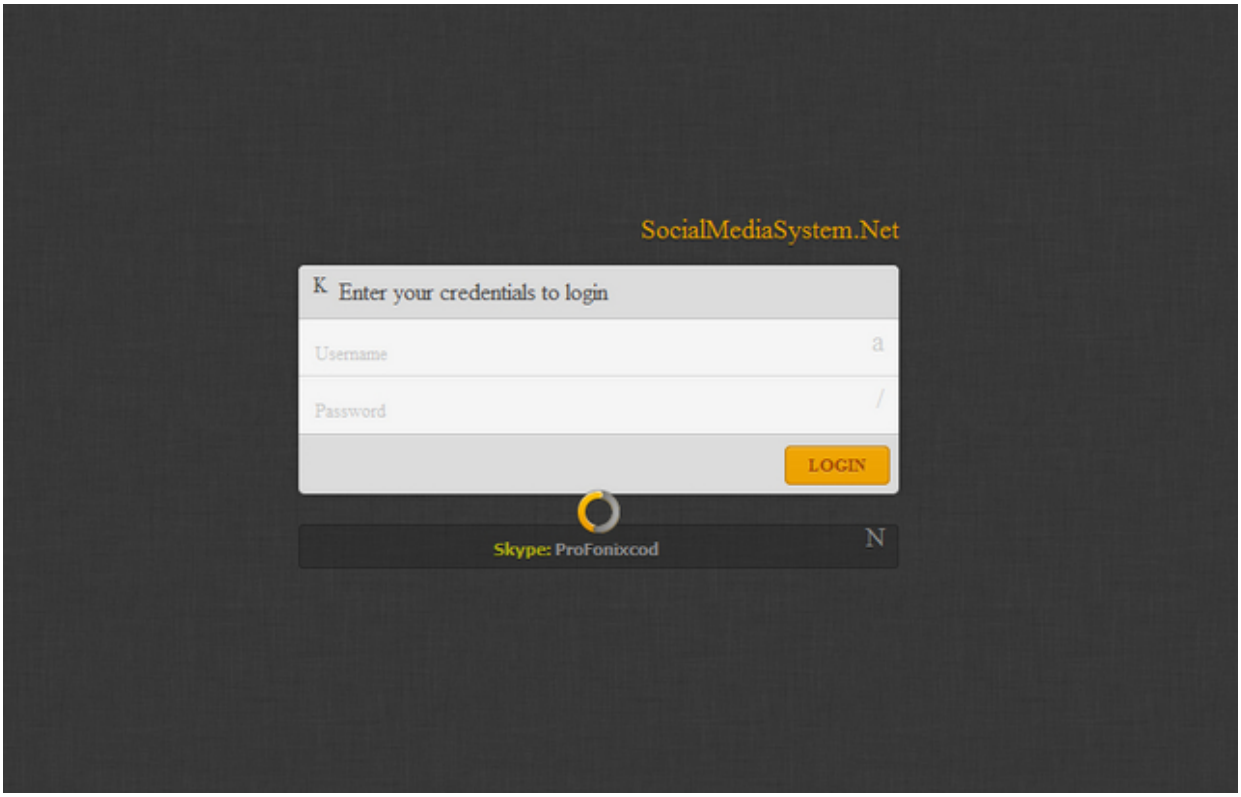
&skin=newtubedark/NewTubeDark.xml &streamer=lighttpd &image=hqdefault.jpg **Domain name reconnaissance:**

hizliservis.pw - Email: furkan@cod.com

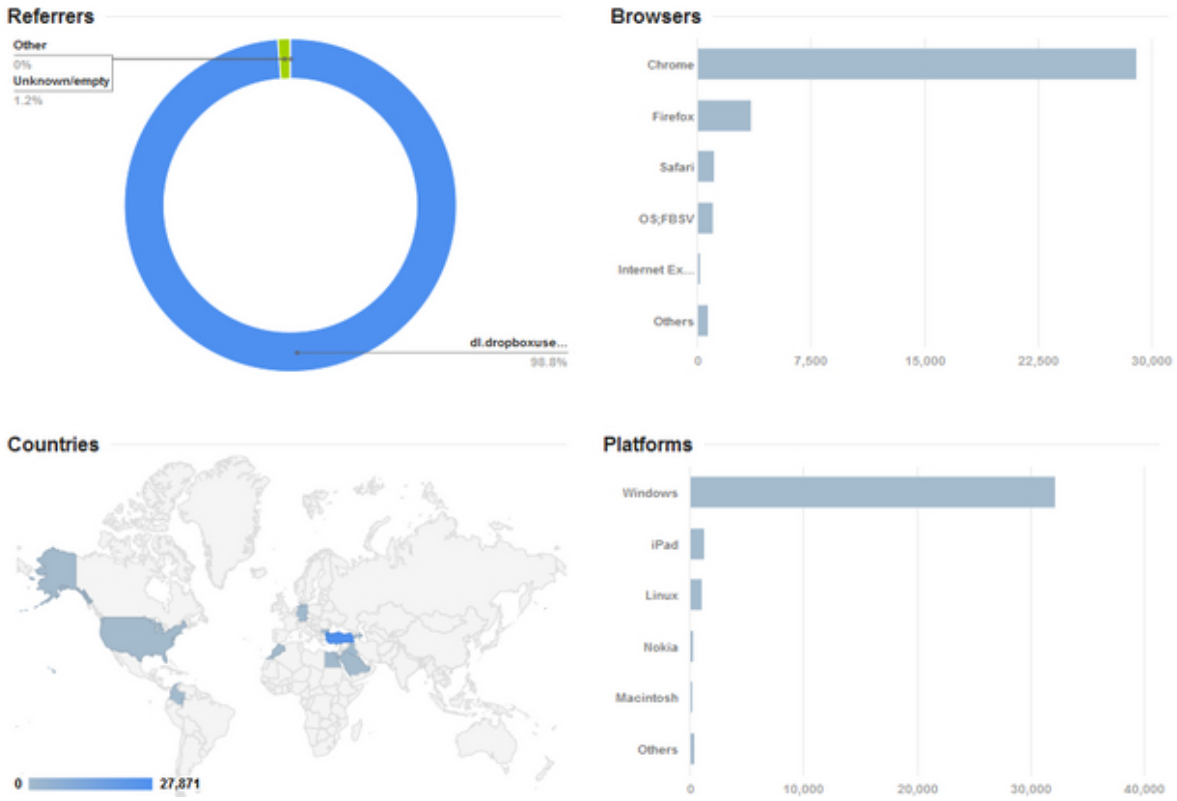
videotr.in - Email: tiiknet@yandex.com; snack@log-z.com

izleyelim.s3.amazonaws.com - 176.32.97.249

Within **hizliservis.pw**, we can easily spot yet another part of the same malicious/fraudulent infrastructure, namely, the rogue social media distribution platform’s login interface.



Sample redirection chain leading to a currently active fake Adobe Flash Player (Win32.Nixofro):
hxxp://socialmediasystem.net/down.php -> hxxps://profonixback31.googlecode.com/svn/FlashPlayer_Guncelle.exe 31



Detection rate for the fake Adobe Flash Player:

[5]**MD5: 28c3c503d398914bdd2c2b3fdc1f9ea4** - detected by 36 out of 50 antivirus scanners as Win32.Nixofro Once executed, the sample phones back to **profonixuser.net** (141.101.117.218) **Known to have responded to the same IP (141.101.117.218) are also the following malicious MD5s:** MD5: 53360155012d8e5c648aca277cbde587

MD5: a66a1c42cc6fb775254cf32c8db7ad5b

MD5: a051fd83fc8577b00d8d925581af1a3b

MD5: f47784817a8a04284af4b602c7719cb7

MD5: 2e5c75318275844ce0ff7028908e8fb4

MD5: 90205a9740df5825ce80229ca105b9e8

Domain name reconnaissance for the rogue social media distibution platform: socialmediasystem.Net (141.101.118.159; 141.101.118.158) - Email: furkan@cod.com **Sample redirection chain for the rogue social media distribution platform's core functions:** *hxxp://profonixuser.net/new.php?nocache=1044379803*

->

hxxp://sosyalmedyakusu.com/oauth.php

(108.162.199.203;

108.162.198.203)

Email:

furkan@cod.com

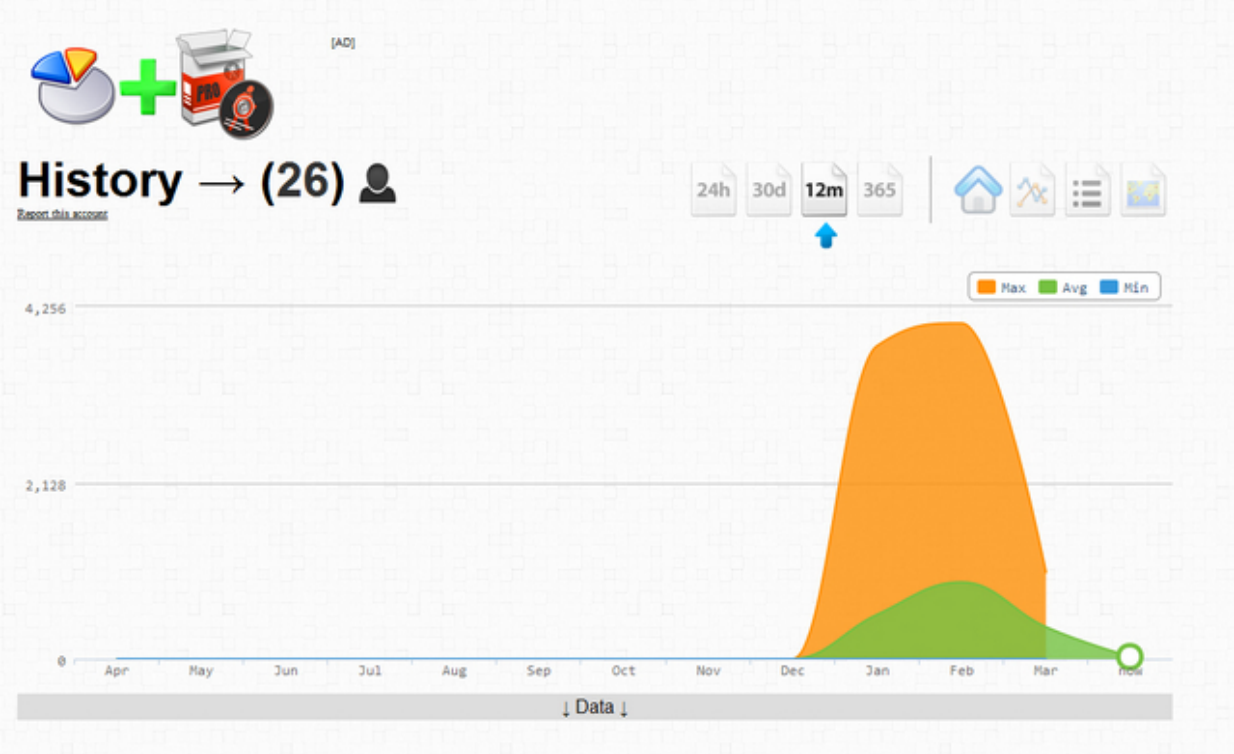
->

hxxp://hizliservis.pw/face.php

->

hxxp://socialhaberler.com/manyak.php -> hxxp://profonixuser.net/new.php -> hxxp://profonixuser.net/amk.php (141.101.117.218) -> *hxxp://me.cf/dhtcw* (31.170.164.67) -> *hxxps://video-players.herokuapp.com/?55517841177*

(107.20.187.159) -> *hxxp://kingprofonix.net/hxxp://kingprofonix.com* (108.162.198.203) the same domain is also known to have responded to 108.162.197.62



Related MD5s known to have phoned back to the same IP (108.162.198.203) in the past:

[6]**MD5: 505f615f9e1c4fdc03964b36ec877d57**

Sample internal redirectors structure:

hxxp://profonixuser.net/fb.php ->
hxxp://profonixuser.net/manyak.php ->
hxxp://molotofcu.com/google/hede.php (199.27.134.199)

->

hxxp://profonixuser.net/pp.php

->

hxxp://gdriv.es/awalbbmprtbpahpolcdt?jgxebgqjl

->

hxxps://googledrive.com/host/0B08vFK4UtN5kdjV2NklHVTVjcTQ -> hxxp://sosyalmedyakusu.com/s3x.php?ref=google

hxxp://profonixuser.net/user.php -> hxxp://goo.gl/ber2EP -> hxxps://buexe-x.googlecode.com/svn/FlashPlayer

%20Setup.exe -> [7]**MD5: 60137c1cb77bed9afcbbbc3ad910df3f** -> phones back to **wjetphp.com** (46.105.56.61) **Secondary sample internal redirectors structure:**

hxxp://profonixuser.net/yarak.txt

->

hxxp://profonixuser.net/u.exe

->

hxxp://profonixuser.net/yeni.txt

-

>

hxxp://profonixuser.net/yeni.exe

->

hxxp://profonixuser.net/recep.html

->

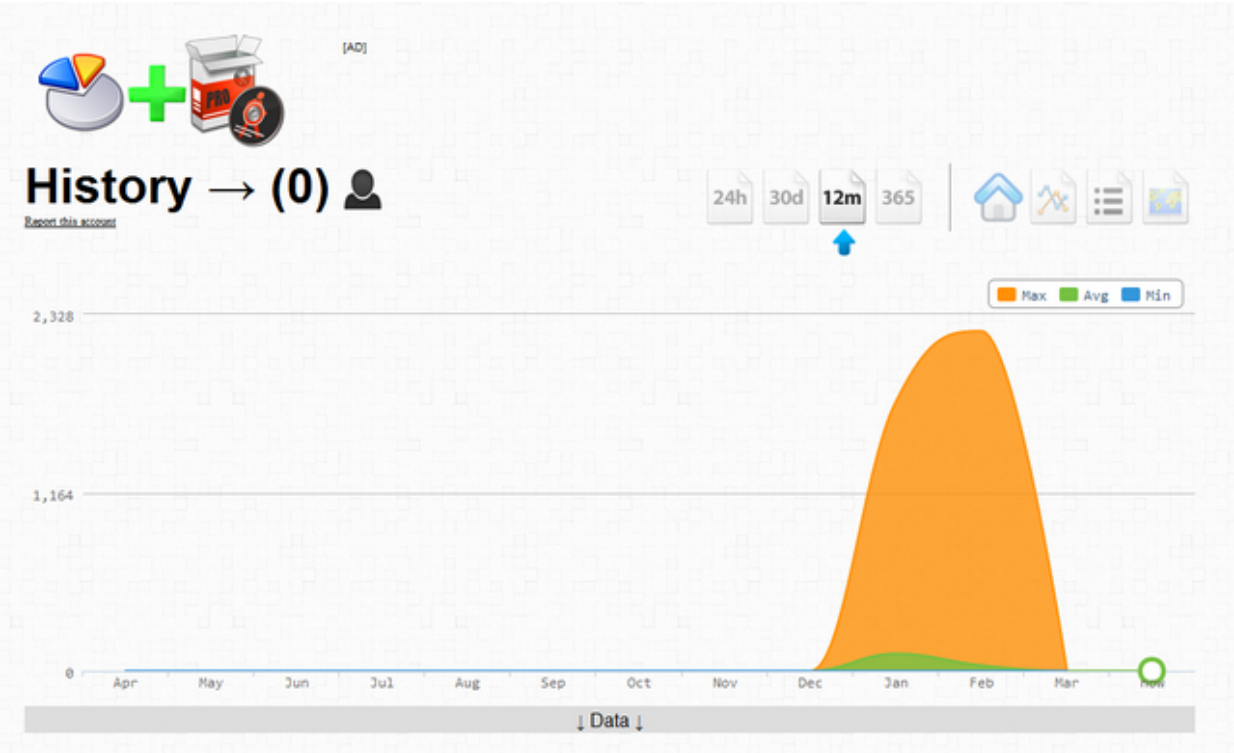
hxxp://goo.gl/ber2EP

->

hxxp://wjetphp.com/unlu/player.swf -> hxxp://profonixuser.net/kral.txt -> hxxp://likef.in/fate.exe -

108.162.194.123; 108.162.195.123; 108.162.199.107 - known to have phoned back to the same IP is also the following malicious [8]**MD5: effcfe91beaf7a3ed2f4ac79525c5fc5** - detected by 35 out of 50 antivirus scanners as Trojan-Ransom.Win32.Foreign.kcme

33

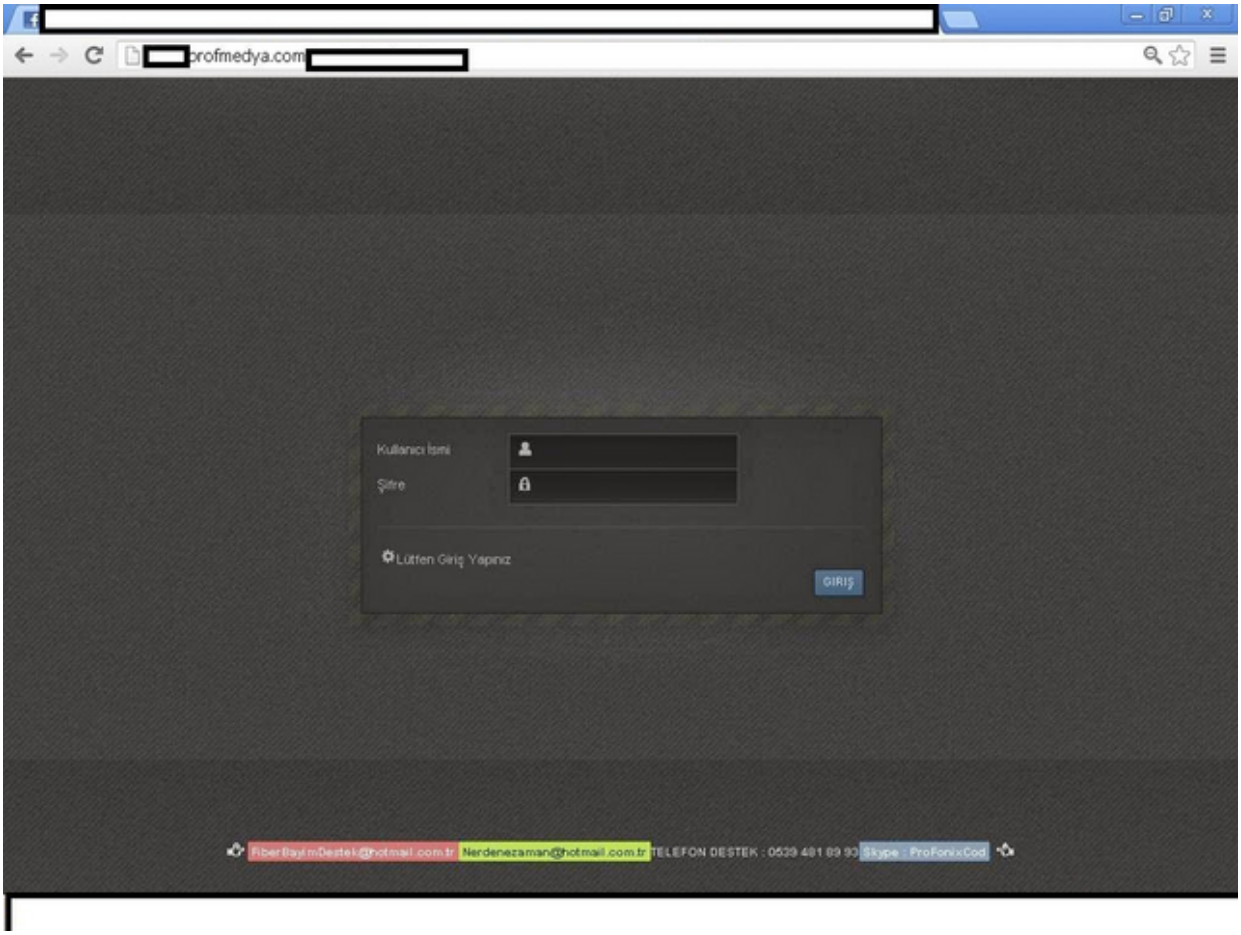


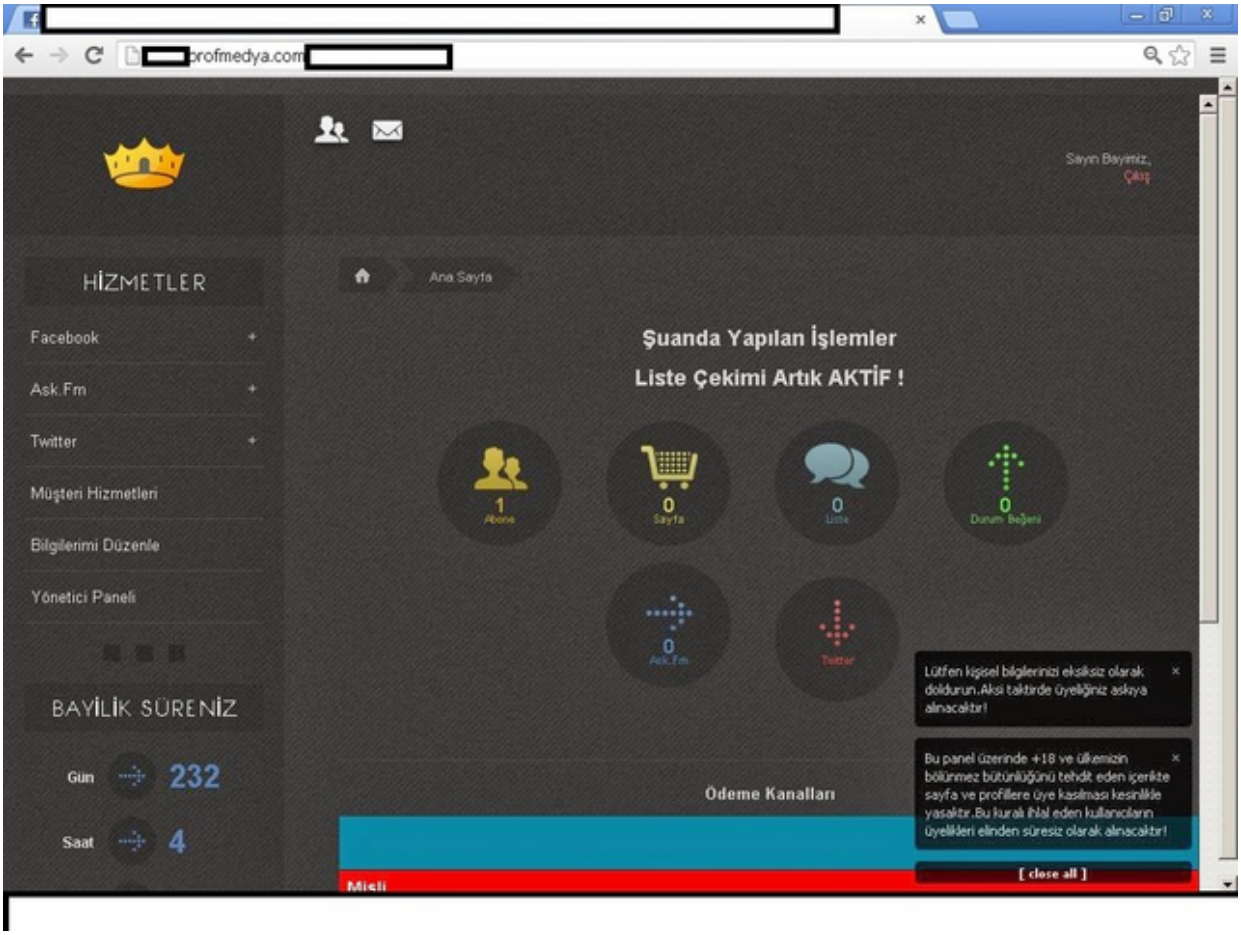
Once executed, the sample phones back to likef.biz (176.53.119.195). The same domain is also known to have responded to the following IPs 141.101.116.165; 141.101.117.165.

Here’s comes the interesting part. The fine folks at [9]**ExposedBotnets**, have already intercepted a malicious Facebook spreading campaign, that’s using the already profiled in this post **videotr.in**.

Having directly connected the cybercrime-friendly SWF iframe/redirector injecting service, with **hizliservis.pw** as well as the SocialMediaSystem as being part of the same malicious infrastructure, it’s time to profile the fraudulent/malicious adversaries behind the campaigns. The cybercriminals behind these campaigns, appear to be operating a rogue social media service, targeting Facebook Inc.

Sample screenshots of the social media distribution platform’s Web based interface: 34





Sample advertisement of the rogue social media distribution platform:

Facebook Page Member Shooting !

1K: 5$
2K: 10$
3K: 15$
4K: 20$
5K: 25$

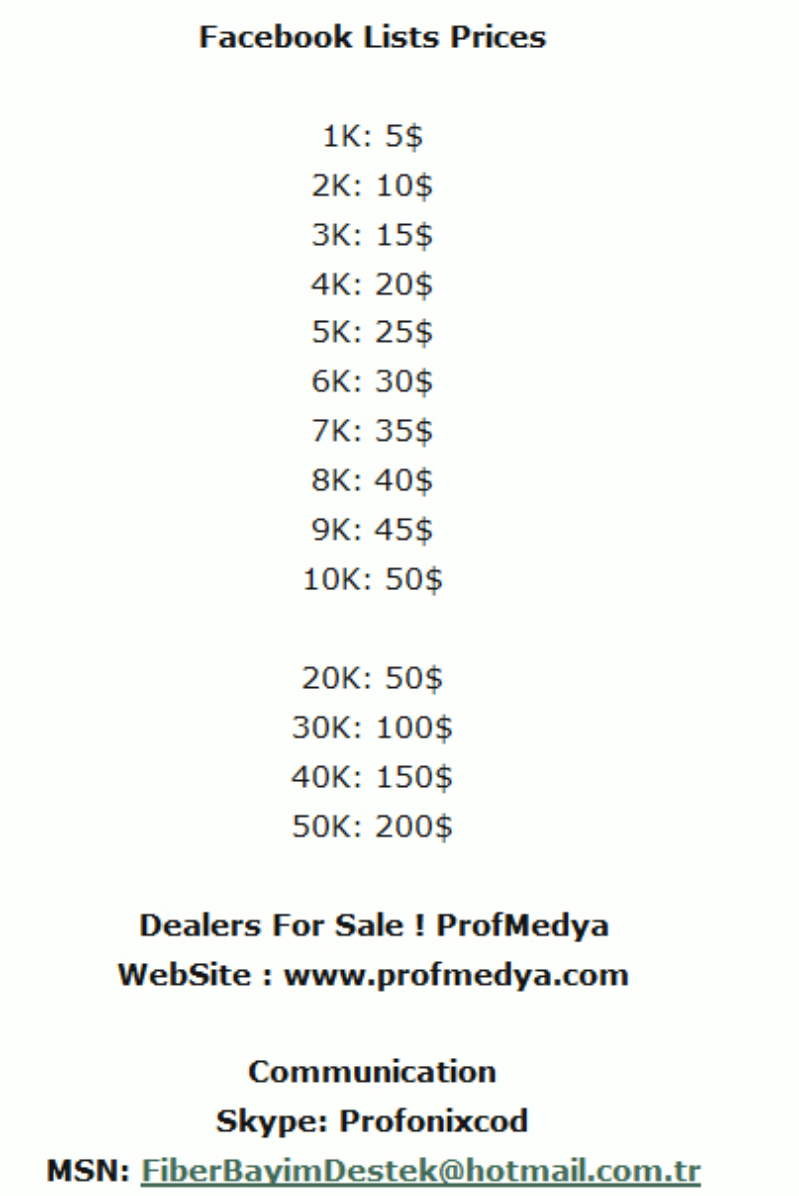
10K: 50$
20K: 100$
30K: 150$
40K: 200$
50K: 250$

Facebook Subscriber Prices

1K: 2$
2K: 5$
3K: 7$
4K: 10$
5K: 12$
6K: 13$
7K: 15$
8K: 17$
9K: 20$
10K: 25$

20K: 50$
30K: 100$
40K: 150$
50K: 200$

Facebook Lists Prices



Skype ID of the rogue company: ProFonixcod

Secondary company name: ProfMedya - hxxp://profmedya.com - 178.33.42.254; 188.138.9.39; 89.19.20.242 - Email: kayahoca@gmail.com. The same domain, profmedya.com used to respond to 188.138.9.39.

Domains known to have responded to the same IP (188.138.9.39) are also the following malicious domains: hxxp://faceblooook.biz

hxxp://worldmedya.net

fhxxp://astotoliked.net

hxxp://adsmedya.com

hxxp://facebookmedya.biz

hxxp://fastotolike.com

hxxp://fbmedyahizmetleri.com

hxxp://fiberbayim.com

hxxp://profonixcoder.com

hxxp://sansurmedya.biz

hxxp://sosyalpaket.com

38

hxxp://takipciniarttir.net

hxxp://videomedya.net

hxxp://videopackage.biz

hxxp://worldmedya.net

hxxp://www–facebook.net

hxxp://www.facebook-java.com

hxxp://www.facemlike.com

hxxp://www.fastcekim.com

hxxp://www.fastotolike.com

hxxp://www.fbmedyahizmetleri.com

hxxp://www.profmedya.com

hxxp://www.sansurmedya.com

Rogue social media distribution platform operator's name: Fatih Konar

Associated emails: fiberbayimdestek@hotmail.com.tr; nerdenezaman@hotmail.com.tr **Google+ Account:** hxxps://plus.google.com/1038477436831294 39807/about

Twitter account: hxxps://twitter.com/ProfonixCodtr

Domain name reconnaissance:

profonixcod.com (profonix-cod.com) - 216.119.143.194 - Email: abazafamily _@hotmail.com (related domains known to have been registered with the same email - warningyoutube.com; likebayi.com) profonixcod.net

Updated will be posted as soon as new developments take place.

1. http://ddanchev.blogspot.com/2014/01/facebook-spreading-amazon.html

2. http://www.webroot.com/blog/2014/02/14/doubleclick-malvertising-campaign-exposes-long-run-beneath-radar-m

alvertising-infrastructure/

3. http://www.webroot.com/blog/2013/06/03/compromised-ftpssh-account-privilege-escalating-mass-iframe-embedd

ing-platform-released-on-the-underground-marketplace/

4. http://www.webroot.com/blog/2012/11/26/cybercriminals-release-stealthy-diy-mass-iframe-injecting-apache-2

-modules/

5. https://www.virustotal.com/en/file/7f7bd5f002de9aedde4fa5dca5356cf576c95eb58bd85178d0781dfc0a1a6ca4/analys

is/1395436639/

6. https://www.virustotal.com/en/file/7aae8f81397608d3c08e3fb645c4001260f560f1470bfbd00ed08cde8ceaedc8/analys

is/

7. https://www.virustotal.com/en/file/4b91da4289b8765d4646176b7fa21f8de515ba02e9751958945 2346d54ff2204/analys

is/

8. https://www.virustotal.com/en/file/a50411aa3850e1defcce38f079daf175a9ca7fb32749c9b4394ef6236476d094/analys

is/

9. http://www.exposedbotnets.com/2014/01/videotrin-facebook-spreading-browser.html

1.2

March

x

Summarizing Webroot's Threat Blog Posts for January (2014-03-06 19:41)

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for January, 2014. You can subscribe to [2]**Webroot's Threat Blog RSS Feed**, or follow me on Twitter:

01. [3]‘Adobe License Service Center Order NR’ and ‘Notice to appear in court’ themed malicious spam campaigns intercepted in the wild

02. [4]New “Windows 8 Home Screen’ themed passwords/game keys stealer spotted in the wild **03.** [5]Vendor of TDoS products resets market life cycle of well known 3G USB modem/GSM/SIM card-based TDoS

tool

04. [6]New TDoS market segment entrant introduces 96 SIM cards compatible custom GSM module, positions itself as market disruptor

05. [7]DIY Python-based mass insecure WordPress scanning/exploting tool with hundreds of pre-defined exploits 41

spotted in the wild

06. [8]Google’s reCAPTCHA under automatic fire from a newly launched reCAPTCHA-solving/breaking service **07.** [9]Fully automated, API-supporting service, undermines Facebook and Google’s ‘SMS/Mobile number activation’

account registration process

08. [10]Newly launched managed ‘compromised/hacked accounts E-shop hosting as service’ standardizes the monetization process

09. [11]Newly released Web based DDoS/Passwords stealing-capable DIY botnet generating tool spotted in the wild **10.** [12]Cybercriminals release new Web based keylogging system, rely on penetration pricing to gain market share

This post has been reproduced from [13]Dancho Danchev's blog . Follow him [14]on Twitter.

1. http://www.webroot.com/blog

2. http://feeds2.feedburner.com/WebrootThreatBlog

3. http://www.webroot.com/blog/2014/01/07/adobe-license-service-center-order-nr-notice-appear-court-themed-malicious-spam-campaigns-intercepted-wild/

4. http://www.webroot.com/blog/2014/01/09/new-windows-8-home-screen-themed-passwordsgame-keys-stealer-spotted-wild/

5. http://www.webroot.com/blog/2014/01/13/vendor-tdos-products-releases-new-gsm3g-usb-modem-based-tdos-tool/

6. http://www.webroot.com/blog/2014/01/16/new-tdos-market-segment-entrant-introduces-96-sim-cards-compatible-custom-gsm-module-positions-market-disruptor/

7. http://www.webroot.com/blog/2014/01/17/diy-python-based-mass-insecure-wordpress-scanningexploting-tool-hundreds-pre-defined-exploits-spotted-wild/

8. http://www.webroot.com/blog/2014/01/21/googles-recaptcha-automatic-fire-newly-launched-recaptcha-solving-breaking-service/

9. http://www.webroot.com/blog/2014/01/22/fully-automated-api-supporting-service-undermines-facebook-googles

-sms-activation-mobile-number-activation-account-regist

10. http://www.webroot.com/blog/2014/01/24/newly-launched-managed-compromisedhacked-accounts-e-shop-hosting-s

ervice-standardizes-monetization-process/

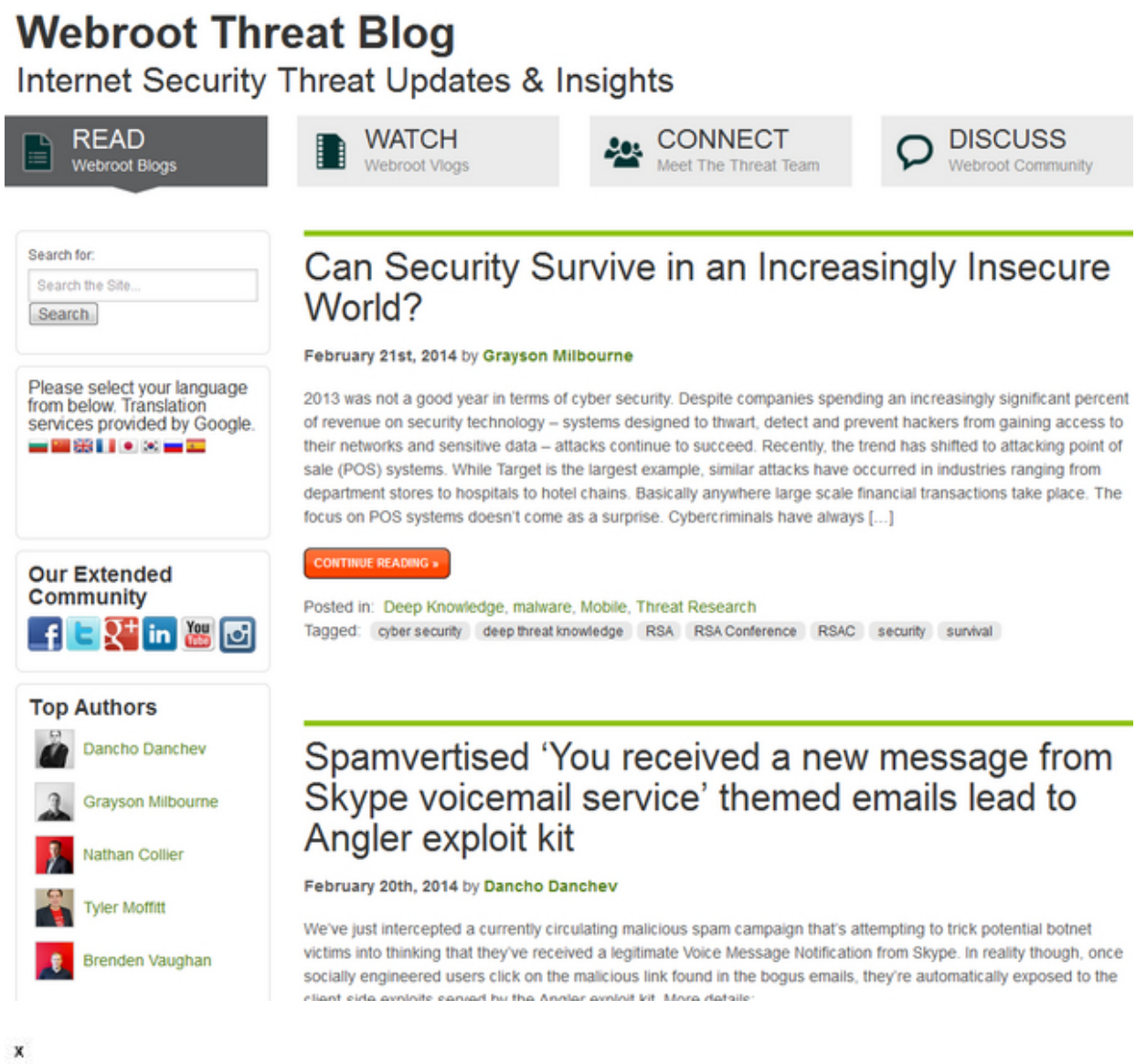
11. http://www.webroot.com/blog/2014/01/30/newly-released-web-based-ddospasswords-stealing-capable-diy-botnet

-generating-tool-spotted-wild/

12. http://www.webroot.com/blog/2014/01/31/cybercriminals-release-new-web-based-keylogging-system/

13. http://ddanchev.blogspot.com/

14. http://twitter.com/danchodanchev



Summarizing Webroot's Threat Blog Posts for February (2014-03-06 20:48)

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for February, 2014. You can subscribe to [2]**Webroot's Threat Blog RSS Feed**, or follow me on Twitter:

01. [3]Cybercriminals release Socks4/Socks5 based Alexa PageRank boosting application **02.** [4]Market leading 'standardized cybercrime-friendly E-shop' service brings

2500+ boutique E-shops online **03.** [5]Managed TeamViewer based anti-forensics capable virtual machines offered as a service **04.** [6]Malicious campaign relies on rogue WordPress sites, leads to client-side exploits through the Magnitude exploit kit

05. [7]‘Hacking for hire’ teams occupy multiple underground market segments, monetize their malicious ‘know how’

06. [8]DoubleClick malvertising campaign exposes long-run beneath the radar malvertising infrastructure **07.** [9]Spamvertised ‘Image has been sent’ Evernote themed campaign serves client-side exploits **08.** [10]Spamvertised ‘You received a new message from Skype voicemail service’ themed emails lead to Angler 43

exploit kit

This post has been reproduced from [11]Dancho Danchev’s blog . Follow him [12]on Twitter.

1. http://www.webroot.com/blog

2. http://feeds2.feedburner.com/WebrootThreatBlog

3.

http://www.webroot.com/blog/2014/02/04/cybercriminals-release-socks4socks5-based-alexa-pagerank-boosting-

application/

4. http://www.webroot.com/blog/2014/02/07/market-leading-standardized-cybercrime-friendly-e-shop-service-bri

ngs-2500-boutique-e-shops-online/

5. http://www.webroot.com/blog/2014/02/10/managed-teamviewer-based-anti-forensics-capable-virtual-machines-offered-service/

6. http://www.webroot.com/blog/2014/02/12/rogue-wordpress-sites-lead-to-client-side-exploits/

7. http://www.webroot.com/blog/2014/02/13/hacking-hire-teams-occupy-multiple-underground-market-segments-monetize-malicious-know/

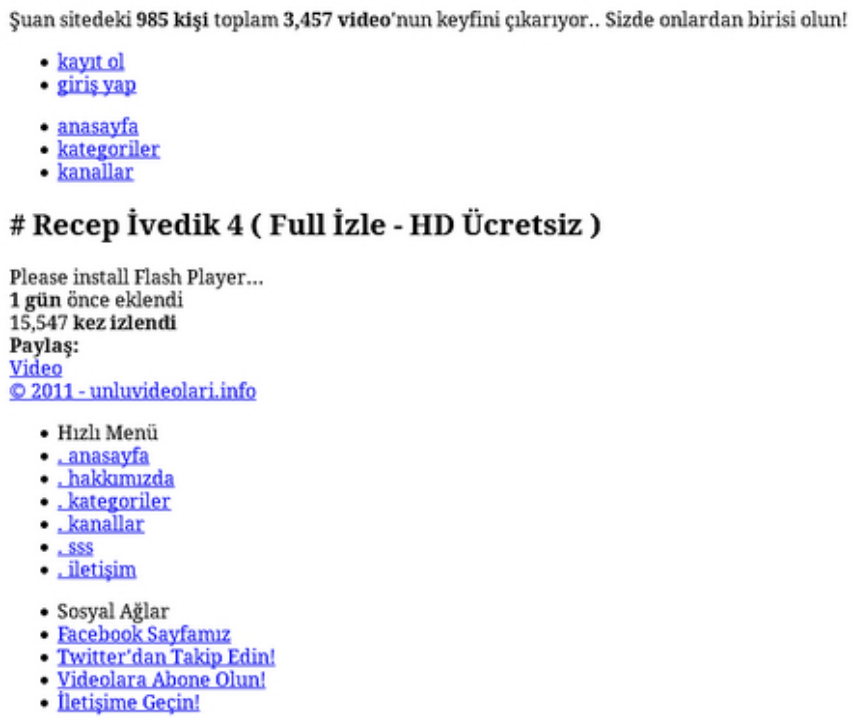
8. http://www.webroot.com/blog/2014/02/14/doubleclick-malvertising-campaign-exposes-long-run-beneath-radar-malvertising-infrastructure/

9. http://www.webroot.com/blog/2014/02/18/spamvertised-image-sent-evernote-themed-campaign-serves-client-side-exploits/

10. http://www.webroot.com/blog/2014/02/20/spamvertised-received-new-message-skype-voicemail-service-themed-emails-lead-angler-exploit-kit/

11. http://ddanchev.blogspot.com/

12. http://twitter.com/danchodanchev


Şuan sitedeki **985 kişi** toplam **3,457 video**'nun keyfini çıkarıyor.. Sizde onlardan birisi olun!

- kayıt ol
- giriş yap

- anasayfa
- kategoriler
- kanallar

 # Recep İvedik 4 (Full İzle - HD Ücretsiz)

Please install Flash Player...
1 gün önce eklendi
15,547 **kez izlendi**
Paylaş:
Video
© 2011 - unluvideolari.info

- Hızlı Menü
- . anasayfa
- . hakkımızda
- . kategoriler
- . kanallar
- . sss
- . iletişim

- Sosyal Ağlar
- Facebook Sayfamız
- Twitter'dan Takip Edin!
- Videolara Abone Olun!
- İletişime Geçin!

Win32.Nixofro Serving, Malicious Infrastructure, Exposes Fraudulent Facebook Social Media Service Provider (2014-03-22 08:18)

I've recently spotted a malicious, cybercrime-friendly SWF iframe/redirector injecting service, that also exposes a long-run Win32.Nixofro serving malicious infrastructure, currently utilized for the purpose of operating a rogue social media service provider, that's targeting Turkish Facebook users through the ubiquitous social engineering vector, for such type of campaigns, namely, the fake Adobe Flash player.

Let's profile the service, discuss its relevance in the broader context of the threat landscape, provide action-able/historical threat intelligene on the malicious infrastructure, the rogue domains involved in it, the

malicious MD5s served by the cybercriminals behind it, and directly link it to a [1]**previously profiled Facebook spreading P2P-Worm.Win32.Palevo serving campaign**.

The managed SWF iframe/redirector service, is a great example of a cybercrime-as-a-service type of underground market proposition, empowering, both, sophisticated and novice cybercriminals with the necessary ([2]**malvertising**)

'know-how', in an efficient manner, directly intersecting with the commercial availability of [3]**sophisticated mass Web site**/[4]**Web server** malicious script embedding platforms.

The managed SWF iframe/redirector injecting service is currently responding to 108.162.197.62 and 108.162.196.62

45

[redacted]	Обычный	Оптовый	VIP персона
Неделя (7 дней)	5	1	0.5
Месяц (30 дней)	10	2	1
Год (365 дней)	15	5	2

Known to have responded to the same IPs (108.162.197.62; 108.162.196.62) is also a key part of the malicious infrastructure that I'll expose in this post, namely **hizliservis.pw** - Email: furkan@cod.com.

Known to have phoned back to the same IP (108.162.197.62) are also the following malicious MD5s: MD5: 432efe0fa88d2a9e191cb95fa88e7b36

MD5: 720ecb1cf4f28663f4ab25eedf620341

MD5: 02691863e9dfb9e69b68f5fca932e729

MD5: 69ed70a82cb35a454c60c501025415aa

MD5: cc586a176668ceef14891b15e1b412ab

MD5: 74291941bddcec131c8c6d531fcb1886

MD5: 7c27d9ff25fc40119480e4fe2c7ca987

MD5: 72c030db7163a7a7bf2871a449d4ea3c

MD5: 432efe0fa88d2a9e191cb95fa88e7b36

Known to have phoned to the same IP (108.162.196.62) are also the following malicious MD5s: MD5: eda3f015204e9565c779e0725915864f

MD5: effcfe91beaf7a3ed2f4ac79525c5fc5

MD5: 14acd831691173ced830f4b51a93e1ca

MD5: 7f93b0c611f7020d28f7a545847b51e0

MD5: bcfce3a9bf2c87dab806623154d49f10

MD5: 4c90a89396d4109d8e4e2491c5da4846

MD5: 289c4f925fdec861c7f765a65b7270af

Sample redirection chain leading to the fake Adobe Flash Player:

hxxp://hizliservis.pw/unlu.htm

->

hxxp://hizliservis.pw/indir.php

->

hxxp://unluvideolari.info

->

hxxp://videotr.in/player.swf

->

hxxp://izleyelim.s3.amazonaws.com/movie.mp4

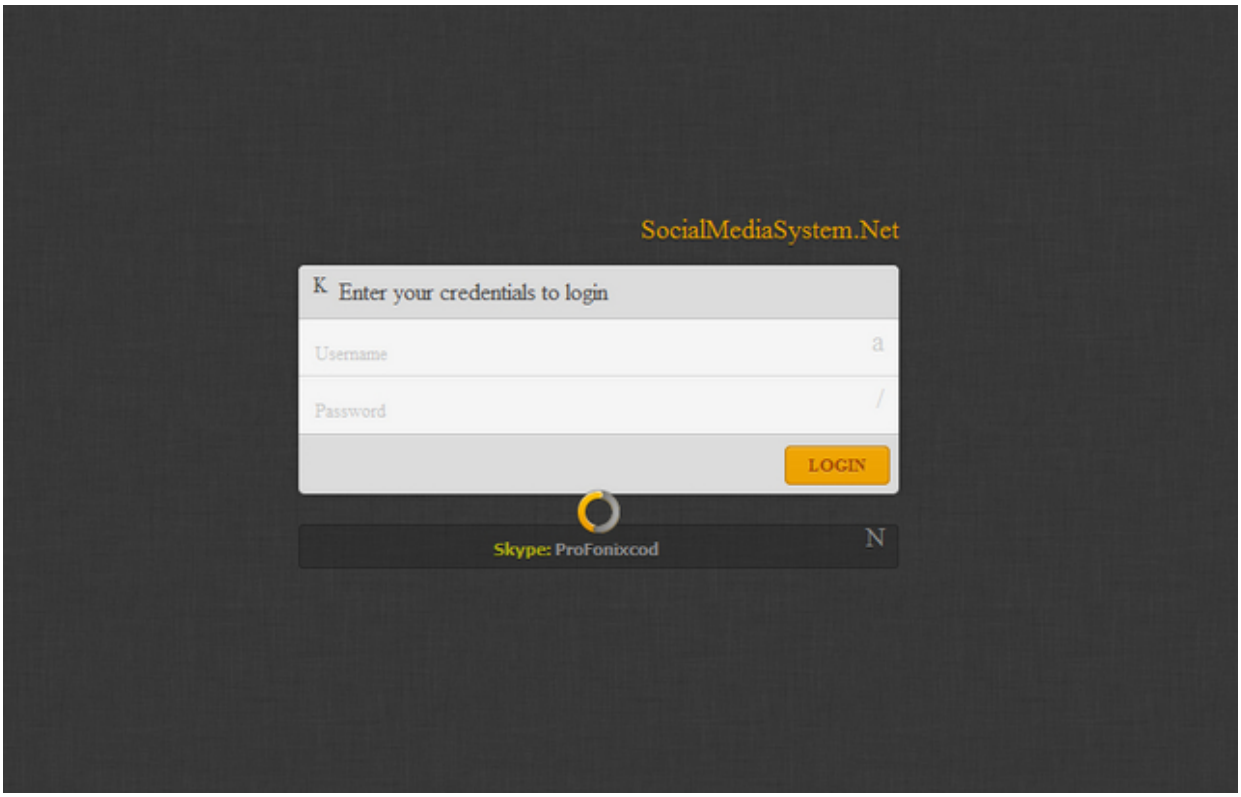
&skin=newtubedark/NewTubeDark.xml &streamer=lighttpd &image=hqdefault.jpg **Domain name reconnaissance:**

hizliservis.pw - Email: furkan@cod.com

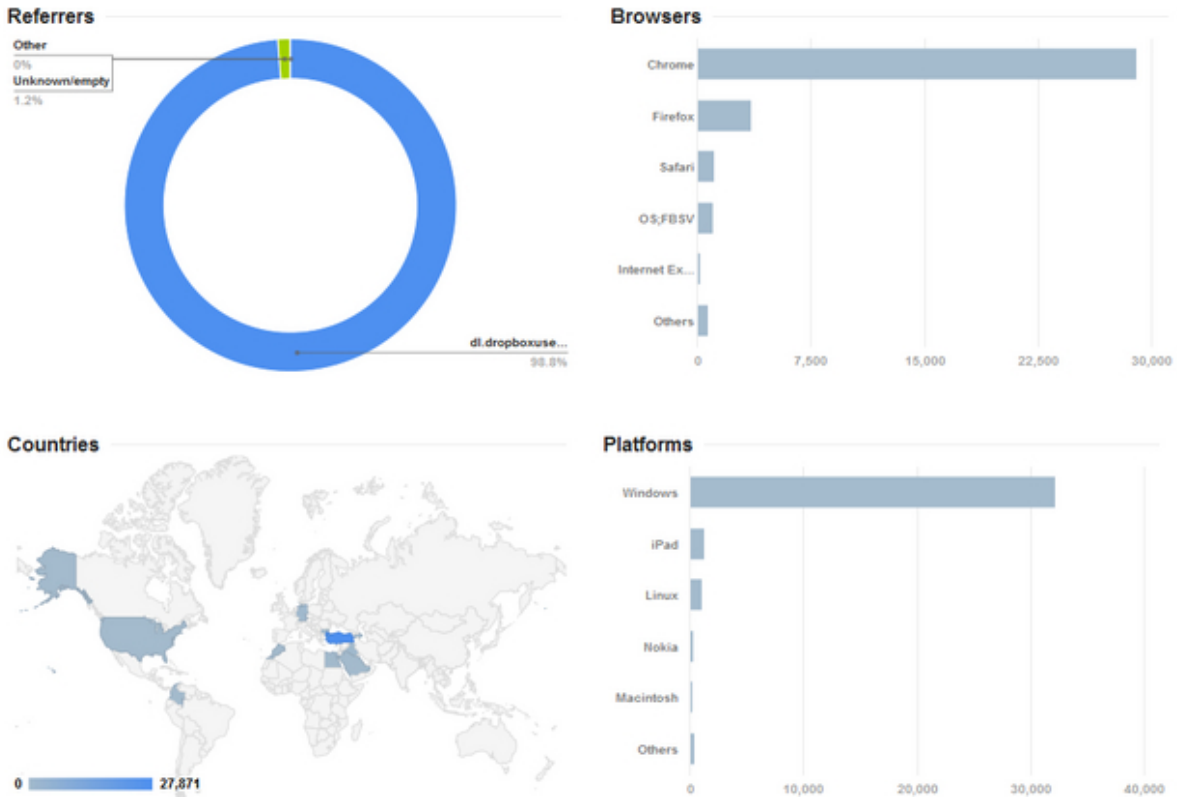
videotr.in - Email: tiiknet@yandex.com; snack@log-z.com

izleyelim.s3.amazonaws.com - 176.32.97.249

Within **hizliservis.pw**, we can easily spot yet another part of the same malicious/fraudulent infrastructure, namely, the rogue social media distribution platform’s login interface.



Sample redirection chain leading to a currently active fake Adobe Flash Player (Win32.Nixofro):
hxxp://socialmediasystem.net/down.php -> hxxps://profonixback31.googlecode.com/svn/FlashPlayer_Guncelle.exe 47



Detection rate for the fake Adobe Flash Player:

[5]**MD5: 28c3c503d398914bdd2c2b3fdc1f9ea4** - detected by 36 out of 50 antivirus scanners as Win32.Nixofro Once executed, the sample phones back to **profonixuser.net** (141.101.117.218) **Known to have responded to the same IP (141.101.117.218) are also the following malicious MD5s:** MD5: 53360155012d8e5c648aca277cbde587

MD5: a66a1c42cc6fb775254cf32c8db7ad5b

MD5: a051fd83fc8577b00d8d925581af1a3b

MD5: f47784817a8a04284af4b602c7719cb7

MD5: 2e5c75318275844ce0ff7028908e8fb4

MD5: 90205a9740df5825ce80229ca105b9e8

Domain name reconnaissance for the rogue social media distibution platform: socialmediasystem.Net (141.101.118.159; 141.101.118.158) - Email: furkan@cod.com **Sample redirection chain for the rogue social media distribution platform's core functions:** *hxxp://profonixuser.net/new.php?nocache=1044379803*

->

hxxp://sosyalmedyakusu.com/oauth.php

(108.162.199.203;

108.162.198.203)

Email:

furkan@cod.com

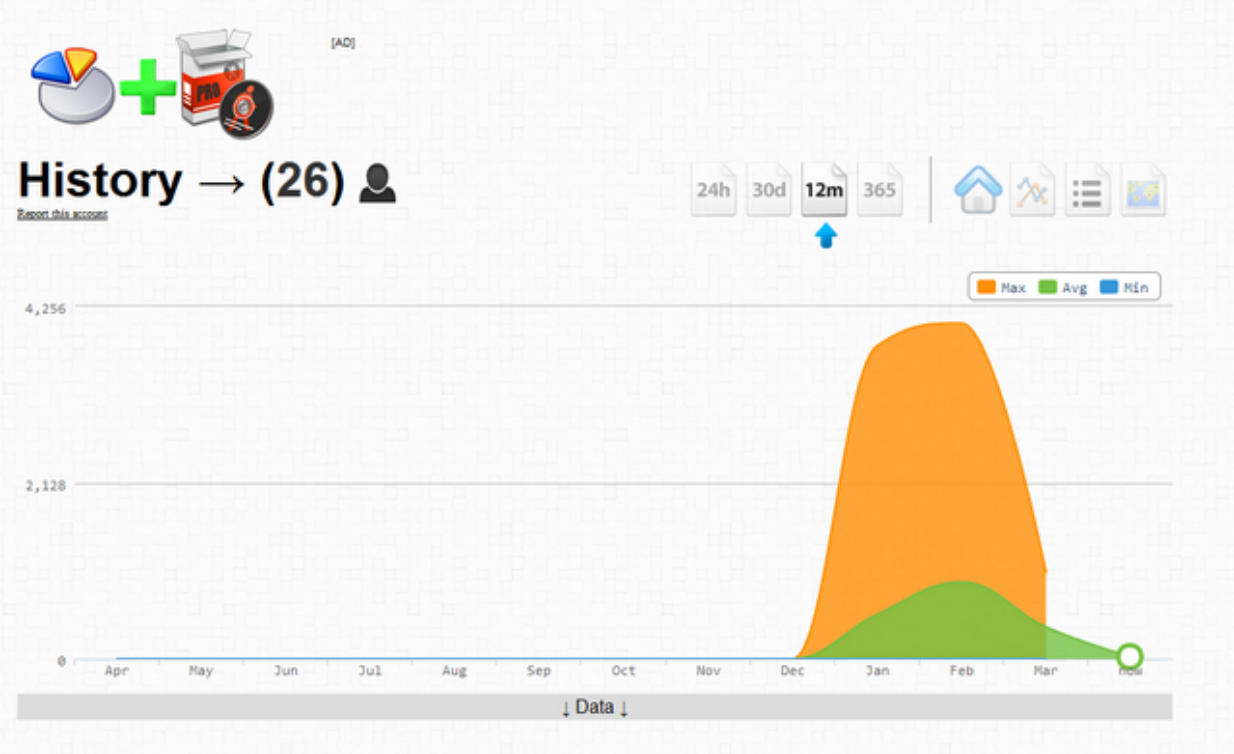
->

hxxp://hizliservis.pw/face.php

->

hxxp://socialhaberler.com/manyak.php -> hxxp://profonixuser.net/new.php -> hxxp://profonixuser.net/amk.php (141.101.117.218) -> *hxxp://me.cf/dhtcw* (31.170.164.67) -> *hxxps://video-players.herokuapp.com/?55517841177*

(107.20.187.159) -> *hxxp://kingprofonix.net/hxxp://kingprofonix.com* (108.162.198.203) the same domain is also known to have responded to 108.162.197.62



Related MD5s known to have phoned back to the same IP (108.162.198.203) in the past:

[6]**MD5: 505f615f9e1c4fdc03964b36ec877d57**

Sample internal redirectors structure:

hxxp://profonixuser.net/fb.php ->
hxxp://profonixuser.net/manyak.php ->
hxxp://molotofcu.com/google/hede.php (199.27.134.199)

->

hxxp://profonixuser.net/pp.php

->

hxxp://gdriv.es/awalbbmprtbpahpolcdt?jgxebgqjl

->

hxxps://googledrive.com/host/0B08vFK4UtN5kdjV2NklHVTVjcTQ -> hxxp://sosyalmedyakusu.com/s3x.php?ref=google

hxxp://profonixuser.net/user.php -> hxxp://goo.gl/ber2EP -> hxxps://buexe-x.googlecode.com/svn/FlashPlayer

%20Setup.exe -> [7]**MD5: 60137c1cb77bed9afcbbbc3ad910df3f** -> phones back to **wjetphp.com** (46.105.56.61) **Secondary sample internal redirectors structure:**

hxxp://profonixuser.net/yarak.txt

->

hxxp://profonixuser.net/u.exe

->

hxxp://profonixuser.net/yeni.txt

-

>

hxxp://profonixuser.net/yeni.exe

->

hxxp://profonixuser.net/recep.html

->

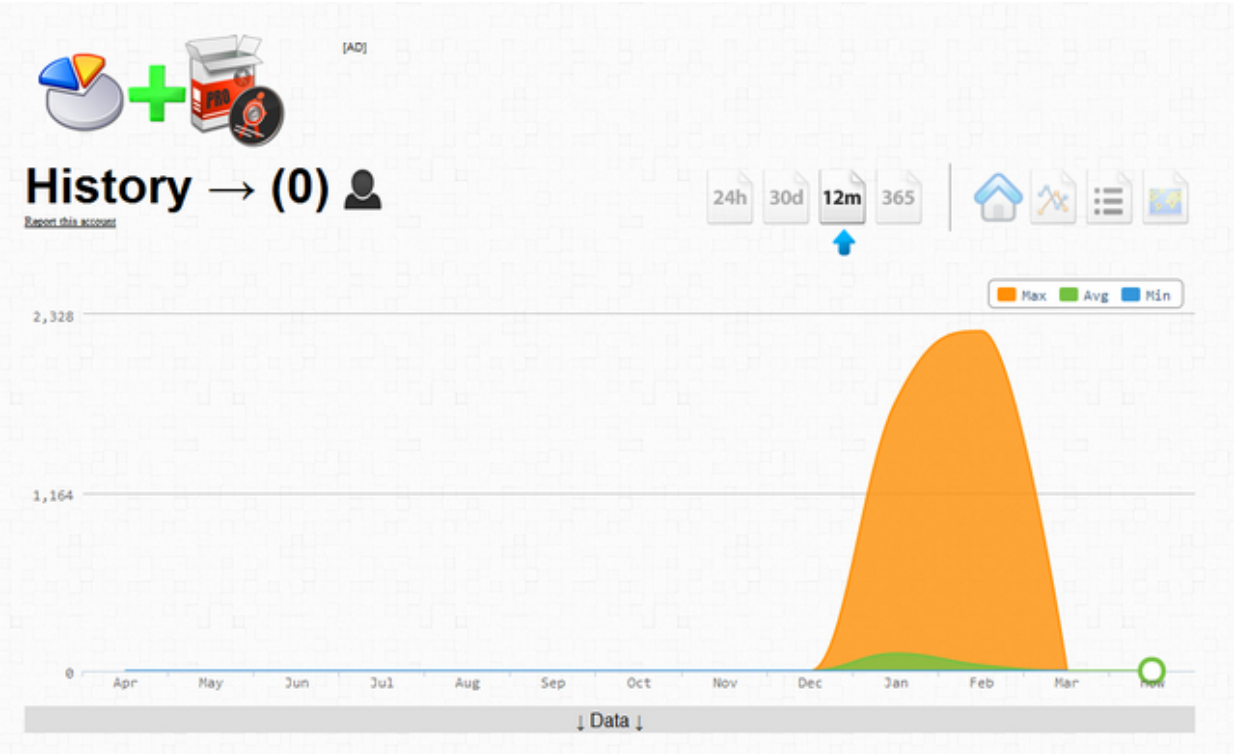
hxxp://goo.gl/ber2EP

->

hxxp://wjetphp.com/unlu/player.swf -> hxxp://profonixuser.net/kral.txt -> hxxp://likef.in/fate.exe -

108.162.194.123; 108.162.195.123; 108.162.199.107 - known to have phoned back to the same IP is also the following malicious [8]**MD5: effcfe91beaf7a3ed2f4ac79525c5fc5** - detected by 35 out of 50 antivirus scanners as Trojan-Ransom.Win32.Foreign.kcme

49

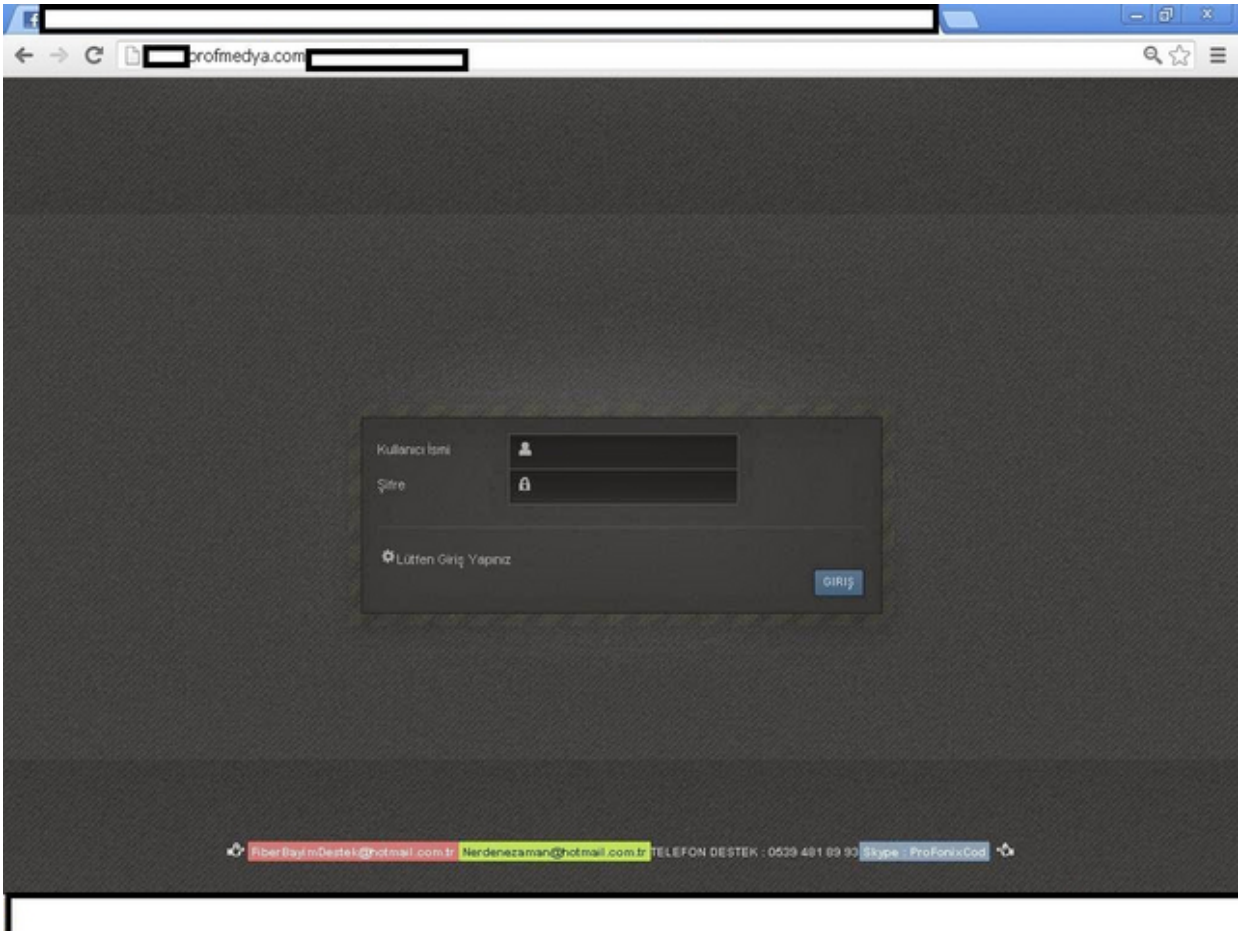


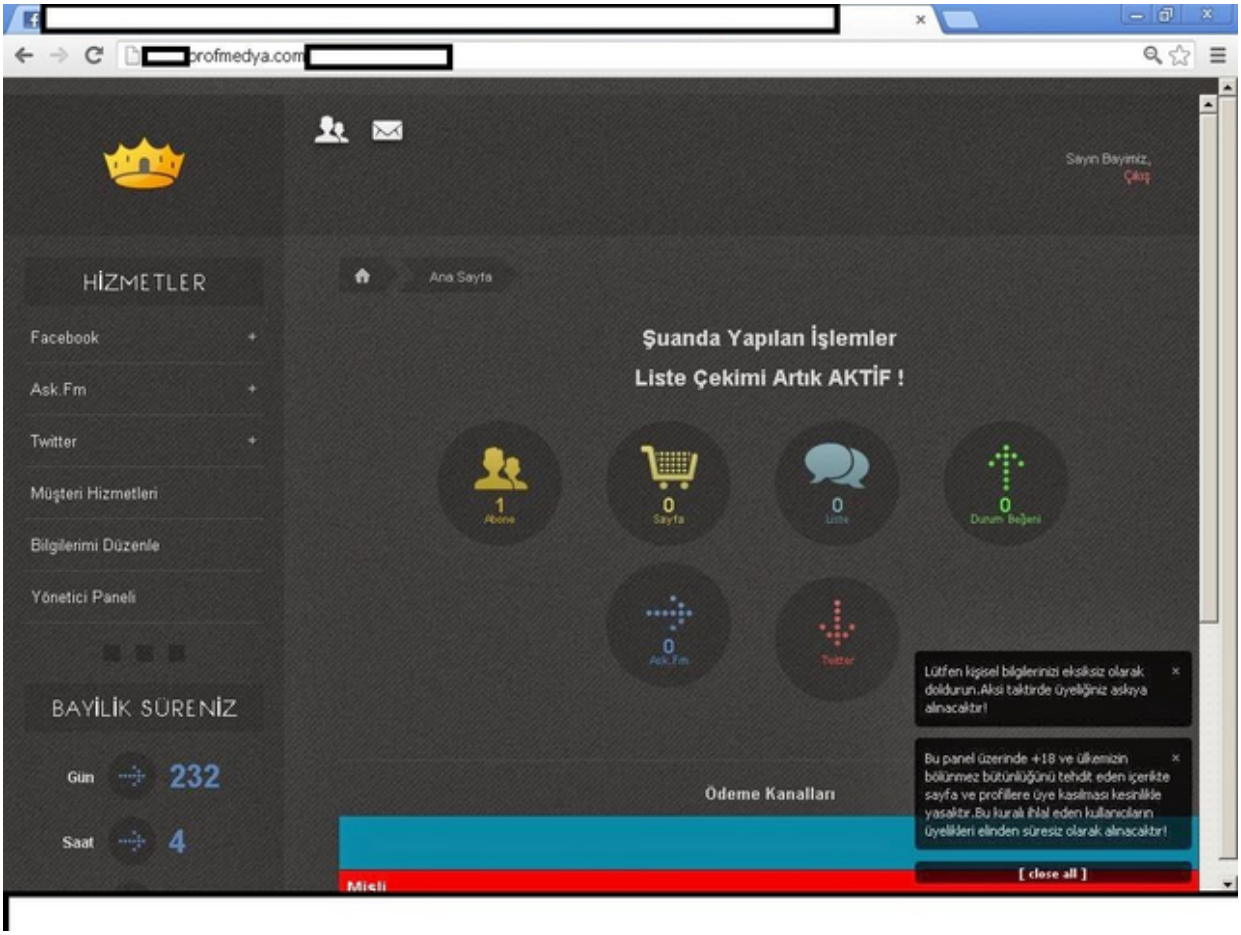
Once executed, the sample phones back to likef.biz (176.53.119.195). The same domain is also known to have responded to the following IPs 141.101.116.165; 141.101.117.165.

Here’s comes the interesting part. The fine folks at [9]**ExposedBotnets**, have already intercepted a malicious Facebook spreading campaign, that’s using the already profiled in this post **videotr.in**.

Having directly connected the cybercrime-friendly SWF iframe/redirector injecting service, with **hizliservis.pw** as well as the SocialMediaSystem as being part of the same malicious infrastructure, it’s time to profile the fraudulent/malicious adversaries behind the campaigns. The cybercriminals behind these campaigns, appear to be operating a rogue social media service, targeting Facebook Inc.

Sample screenshots of the social media distribution platform’s Web based interface: 50





Sample advertisement of the rogue social media distribution platform:

Facebook Page Member Shooting !

1K: 5$
2K: 10$
3K: 15$
4K: 20$
5K: 25$

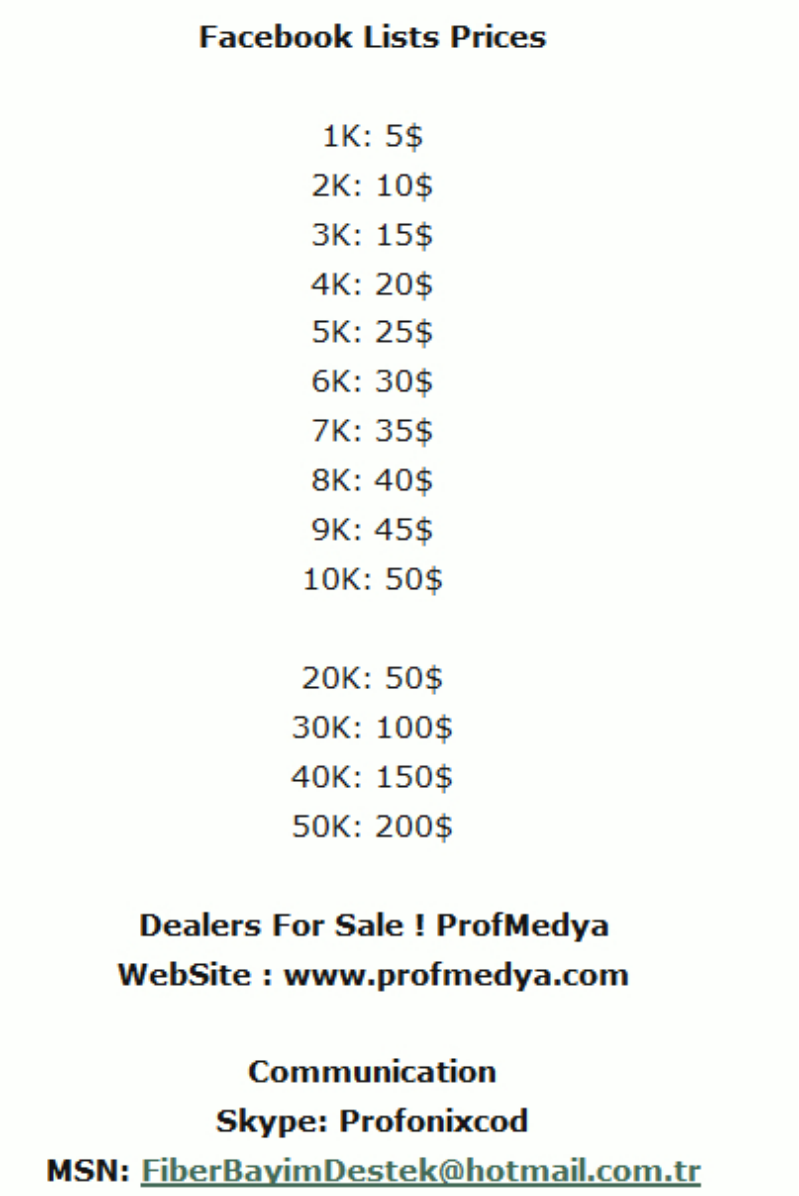
10K: 50$
20K: 100$
30K: 150$
40K: 200$
50K: 250$

Facebook Subscriber Prices

1K: 2$
2K: 5$
3K: 7$
4K: 10$
5K: 12$
6K: 13$
7K: 15$
8K: 17$
9K: 20$
10K: 25$

20K: 50$
30K: 100$
40K: 150$
50K: 200$

Facebook Lists Prices



Skype ID of the rogue company: ProFonixcod

Secondary company name: ProfMedya - hxxp://profmedya.com - 178.33.42.254; 188.138.9.39; 89.19.20.242 - Email: kayahoca@gmail.com. The same domain, profmedya.com used to respond to 188.138.9.39.

Domains known to have responded to the same IP (188.138.9.39) are also the following malicious domains: hxxp://faceblooook.biz

hxxp://worldmedya.net

fhxxp://astotoliked.net

hxxp://adsmedya.com

hxxp://facebookmedya.biz

hxxp://fastotolike.com

hxxp://fbmedyahizmetleri.com

hxxp://fiberbayim.com

hxxp://profonixcoder.com

hxxp://sansurmedya.biz

hxxp://sosyalpaket.com

54

hxxp://takipciniarttir.net

hxxp://videomedya.net

hxxp://videopackage.biz

hxxp://worldmedya.net

hxxp://www–facebook.net

hxxp://www.facebook-java.com

hxxp://www.facemlike.com

hxxp://www.fastcekim.com

hxxp://www.fastotolike.com

hxxp://www.fbmedyahizmetleri.com

hxxp://www.profmedya.com

hxxp://www.sansurmedya.com

Rogue social media distribution platform operator's name: Fatih Konar

Associated emails: fiberbayimdestek@hotmail.com.tr; nerdenezaman@hotmail.com.tr **Google+ Account:** hxxps://plus.google.com/1038477436831294 39807/about

Twitter account: hxxps://twitter.com/ProfonixCodtr

Domain name reconnaissance:

profonixcod.com (profonix-cod.com) - 216.119.143.194 - Email: abazafamily _@hotmail.com (related domains known to have been registered with the same email - warningyoutube.com; likebayi.com) profonixcod.net

Updated will be posted as soon as new developments take place.

1. http://ddanchev.blogspot.com/2014/01/facebook-spreading-amazon.html

2. http://www.webroot.com/blog/2014/02/14/doubleclick-malvertising-campaign-exposes-long-run-beneath-radar-m

alvertising-infrastructure/

3. http://www.webroot.com/blog/2013/06/03/compromised-ftpssh-account-privilege-escalating-mass-iframe-embedd

ing-platform-released-on-the-underground-marketplace/

4. http://www.webroot.com/blog/2012/11/26/cybercriminals-release-stealthy-diy-mass-iframe-injecting-apache-2

-modules/

5. https://www.virustotal.com/en/file/7f7bd5f002de9aedde4fa5dca5356cf576c95eb58bd85178d0781dfc0a1a6ca4/analysis/1395436639/

6. https://www.virustotal.com/en/file/7aae8f81397608d3c08e3fb645c4001260f560f1470bfbd00ed08cde8ceaedc8/analysis/

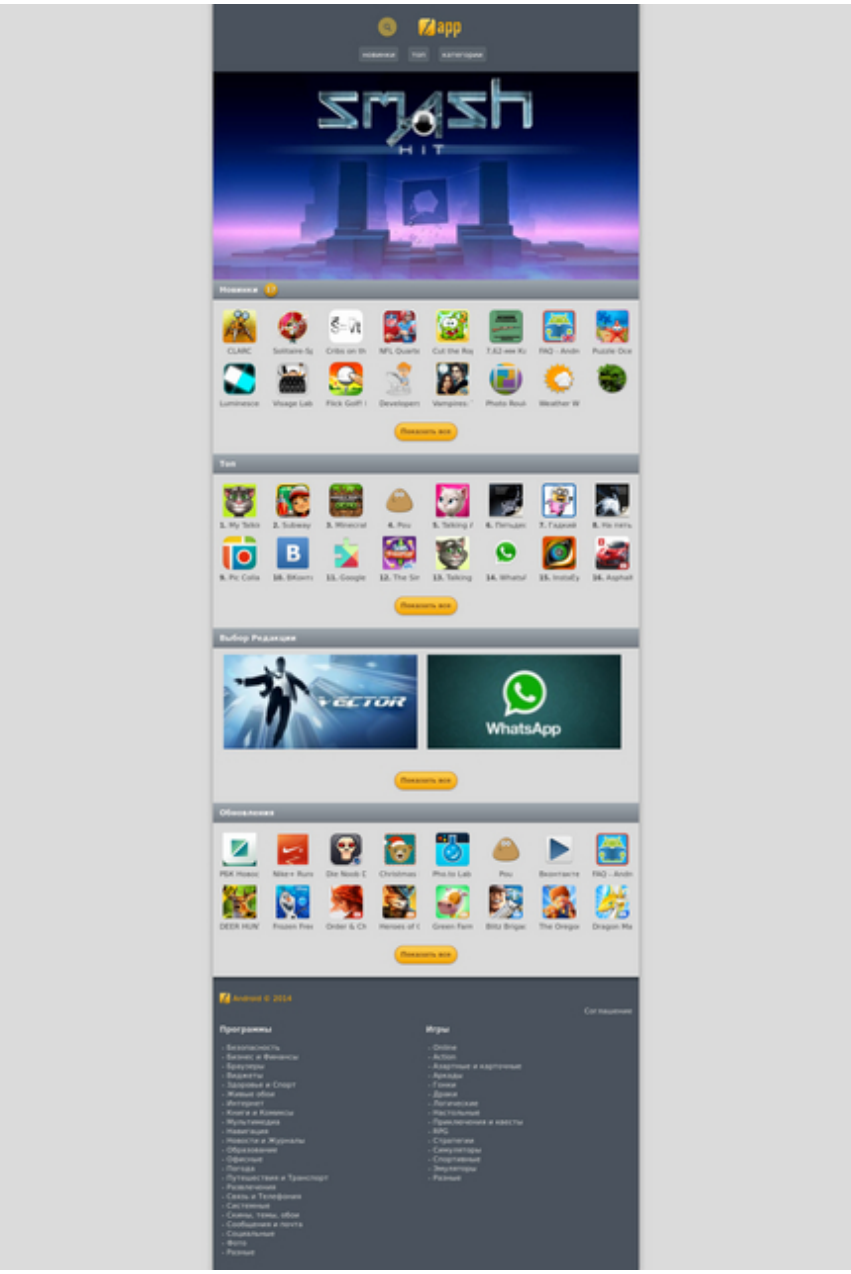
7. https://www.virustotal.com/en/file/4b91da4289b8765d4646176b7fa21f8de515ba02e9751958945234 6d54ff2204/analysis/

8. https://www.virustotal.com/en/file/a50411aa3850e1defcce38f079daf175a9ca7fb32749c9b4394ef6236476d094/analysis/

9. http://www.exposedbotnets.com/2014/01/videotrin-facebook-spreading-browser.html

1.3

October



Rogue Android Apps Hosting Web Site Exposes Malicious Infrastructure (2014-10-21 21:24) With cybercriminals continuing to populate the cybercrime ecosystem with automatically generated and monetized mobile malware variants, we continue to observe a logical shift towards convergence of [1]**cybercrime-friendly revenue sharing affiliate networks**, and [2]**malicious**

infrastructure providers, on their way to further achieve a posive ROI (return on investment) out of their [3]**risk-forwarding fraudulent activities**.

I've recently spotted a legitimately looking, [4]**rogue Android apps hosting Web site**, directly connected to a market leading [5]**DIY API-enabled mobile malware generating/monetizing platform**, further exposing related

[6]**fraudulent operations**, performed, while utilizing the [7]**malicious infrastructure**, which I'll expose in this post.

Let's assess the campaign, expose the malicious infrastructure behind it, list the cybercrime-friendly premium rate SMS numbers, involved in it, as well as related malicious MD5s, known to have participated in the campaign/have utilized the same malicious infrastructure.

57

Sample rogue Android apps hosting URL: *hxxp://androidapps.mob.wf* - 37.1.206.173

Responding to the same IP (37.1.206.173) are also the following fraudulent domains: *hxxp://22-minuty.ru*

hxxp://nygolfpro.com

hxxp://bloomster.dp.ua

hxxp://stdstudio.com.ua

hxxp://autosolnce.ru

Detection rate for sample rogue Android apps:

[8]MD5: 4bf349b601fd73c74eafc01ce8ea8be7

[9]MD5: c4508c127029571e5b6f6b08e5c91415

[10]MD5: bd296d35bf41b9ae73ed816cc7c4c38b

Sample

redirection

chain

exposing

the

fraudulent

infrastructure:

hxxp://22-minuty.ru

->

hxxp://playersharks2.com/player.php/?userid= - 94.242.214.133; 94.242.214.155

Known to have responded to the same IPs (94.242.214.133; 94.242.214.155) are also the following fraudulent domains, participating in a related revenue-sharing affiliate network based type of monetization scheme: *hxxp://4books.ru*

hxxp://annoncer.media-bar.ru

hxxp://booksbutton1.com

hxxp://film-club.ru

hxxp://film-popcorn.ru

hxxp://filmbuttons.ru

hxxp://filmi-doma.com

hxxp://filmonika.ru

hxxp://films.909.su

hxxp://indiiskie.ru

hxxp://kinozond.ru

hxxp://media-bar.ru

hxxp://playersharks2.com

hxxp://playersharks4.com

hxxp://pplayer.ru

hxxp://sharksplayer2.com

hxxp://sharksplayer3.ru

hxxp://sharksreader.ru

hxxp://tema-info.ru

hxxp://toppfilms.ru

hxxp://video-movies.com

hxxp://video.909.su

hxxp://videodomm.ru

hxxp://videozzy.com

hxxp://videozzzz.ru

hxxp://websharks.ru

hxxp://yasmotrju.ru

58

Malicious MD5s known to have phoned back to the same IP (94.242.214.133):

MD5: 9ec8aef6dc0e3db8596ac54318847328

MD5: 895c38ec4fb1fbee47bfb3b6ee3a170b

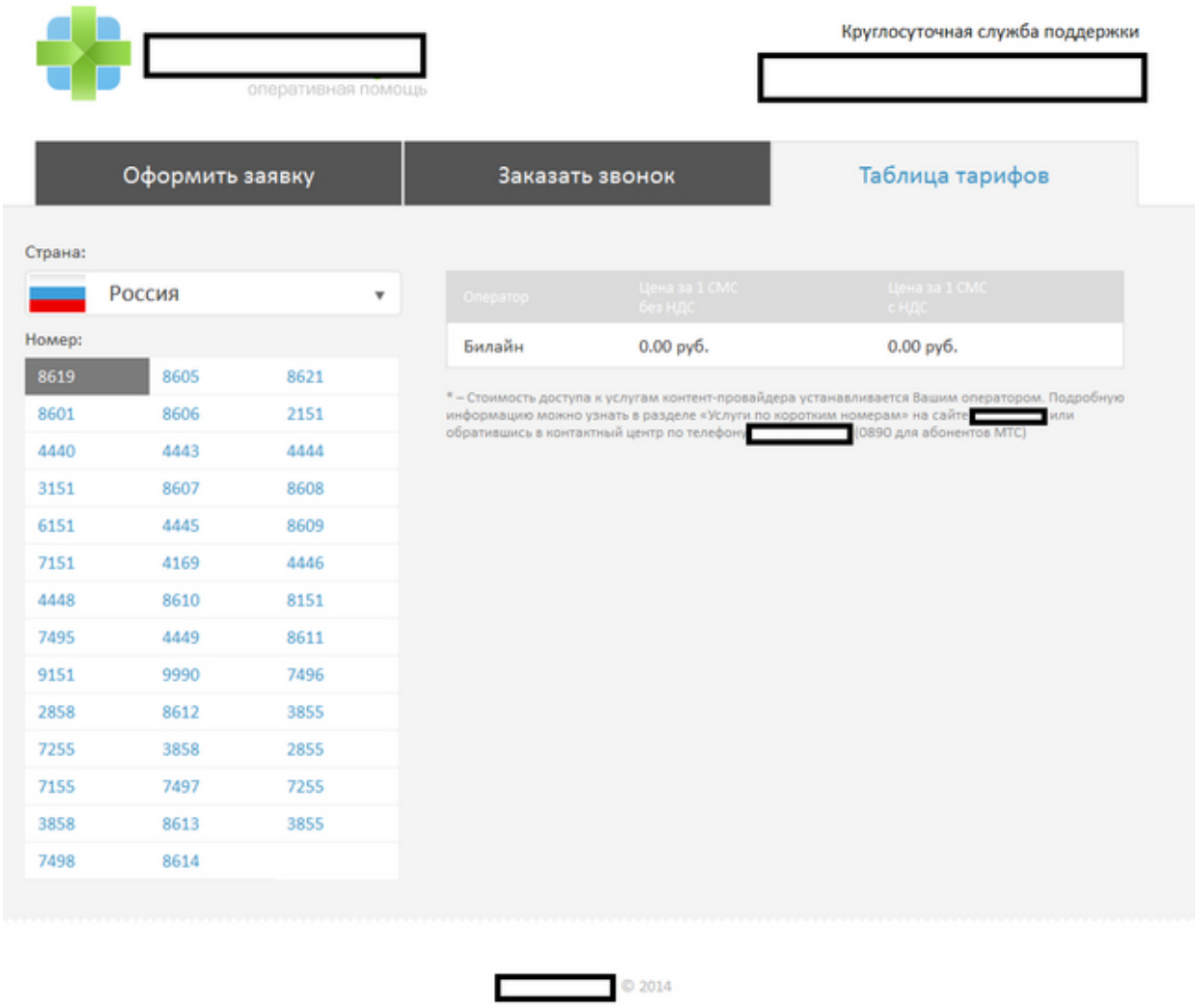
MD5: c4d88b32b605500b7f86de5569a11e22

MD5: 49861fd4748dd57c192139e8bd5b71e3

MD5: 8b350f8a32ef4b28267995cf8f0ceae1

Premium rate SMS numbers involved in the fraudulent scheme:

7151; 9151; 2855; 3855; 3858; 2858; 8151; 7155; 7255; 3190; 3200; 3170; 3006; 3150; 6150; 4124; 4481; 7781; 5014; 1151; 4125; 1141; 1131; 1350; 3354; 7122; 3353; 7132; 3352; 8355; 8155; 8055; 7515; 1037; 1953; 3968; 5370; 1952; 3652; 5373; 9191; 1005; 7019; 7250; 1951; 7015; 7099; 7030



Once executed MD5: 9ec8aef6dc0e3db8596ac54318847328 phones back to the following C &C servers, further exposing the malicious infrastructure:

67.215.246.10:6881

82.221.103.244:6881

114.252.58.66:6407

89.136.77.86:45060

212.25.54.183:32822

107.191.223.72:22127

87.89.149.106:24874

82.247.154.128:47988

108.181.68.73:47342

82.74.179.126:52352

121.222.168.146:64043

217.121.30.46:34421

115.143.245.78:51548

110.15.205.16:51477

37.114.69.97:19079

60

85.229.206.243:55955

95.109.112.178:60018

95.68.195.182:44025

239.192.152.143:6771

109.187.54.101:13100

117.194.5.97:55535

95.29.112.178:59039

109.162.133.97:19459

83.205.112.178:11420

95.68.3.182:53450

175.115.103.140:52696

197.2.133.97:27334

84.55.8.7:10060

27.5.132.243:19962

123.109.176.178:36527

175.157.176.178:22906

188.187.147.247:14745

178.212.133.205:52416

145.255.1.250:41973

213.21.32.190:51413

93.73.165.31:61889

176.97.214.119:46605

185.51.127.134:16447

109.239.42.123:16845

77.232.158.215:40266

178.173.37.2:47126

62.84.24.219:47594

37.144.87.15:13448

5.251.28.179:39620

94.19.66.51:42894

94.51.242.89:35691

93.179.102.216:24458

212.106.62.201:44821

95.52.69.39:12249

46.118.64.45:44172

217.175.33.130:45244

185.8.126.226:32972

93.92.200.202:56664

94.214.220.37:35196

46.182.132.67:32103

46.188.123.131:11510

83.139.188.142:34549

188.232.124.16:27582

91.213.23.226:19751

95.32.142.28:55555

95.83.188.157:15714

95.128.244.10:59239

176.31.240.170:6882

79.109.88.241:6881

91.215.90.109:34600

61

62.198.229.165:6881

91.148.118.250:21558

81.82.210.40:6881

97.121.23.163:31801

78.186.155.62:6881

78.1.158.105:47475

79.160.62.185:9005

213.87.123.81:17790

178.150.154.26:26816

83.174.247.71:59908

109.87.175.144:29374

86.57.186.171:45013

193.222.140.60:35691

176.115.158.138:24253

42.98.191.90:7085

178.127.152.72:10107

82.239.74.201:61137

185.19.22.192:46337

86.185.92.38:10819

78.214.194.145:24521

37.78.85.173:49001

82.70.112.150:32371

37.131.212.35:18525

79.136.156.151:59659

2.134.48.150:12530

95.29.164.86:6881

37.147.16.242:64954

79.45.36.86:22690

112.208.182.65:56374

62.99.29.74:44822

95.16.12.111:12765

124.169.69.69:41216

5.164.83.49:62348

79.22.73.216:61914

46.63.131.146:6881

89.150.119.203:55029

58.23.49.24:2717

83.41.5.241:45624

87.21.80.23:27949

178.150.176.150:57997

178.127.195.146:58278

5.141.236.13:15784

125.182.35.138:54094

99.228.23.82:29302

14.111.131.146:33433

122.177.90.137:25375

178.223.195.146:54596

182.54.112.150:1058

109.23.145.152:31514

213.241.204.31:27769

62

188.168.58.6:45823

2.94.4.215:50830

42.91.39.236:13923

116.33.113.4:19973

86.182.170.27:25712

177.82.206.231:39043

122.143.152.35:7890

217.13.219.147:39190

77.75.13.195:16279

87.239.5.144:58749

89.141.116.97:49001

176.106.11.49:44690

112.14.110.199:33243

122.26.6.52:20527

178.223.195.146:23034

98.118.85.85:51413

190.63.131.146:6881

46.151.242.82:16046

176.106.19.185:46114

85.113.157.12:62633

192.168.0.105:58749

211.89.227.34:56333

36.68.16.149:42839

31.15.80.10:42061

130.15.95.112:6881

87.119.245.51:6882

109.173.101.19:19700

193.93.187.234:1214

176.106.18.254:43469

176.183.137.53:19155

176.113.168.51:52672

93.123.60.130:52981

79.100.9.81:14053

91.124.125.16:29914

46.16.228.135:53473

95.61.55.234:22974

190.213.101.39:44376

58.173.158.99:50821

188.25.108.102:31047

95.153.175.173:15563

75.120.194.116:58001

61.6.218.126:63291

128.70.19.98:64296

5.167.193.5:25861

185.57.73.27:47892

109.205.249.105:58449

77.228.235.226:57715

2.62.49.161:49001

67.234.161.61:65228

91.243.100.237:40431

63

105.155.1.67:16084

73.34.178.71:41864

145.255.169.122:4612

92.241.241.4:61613

145.255.21.166:46596

83.253.71.148:34016

173.246.26.126:12988

79.181.115.213:43853

46.237.69.97:50772

86.159.67.146:48959

213.100.105.54:52147

178.45.129.126:45710

188.78.232.53:39336

70.82.20.41:11248

88.132.82.254:52722

85.198.154.126:35403

89.67.245.2:21705

95.76.128.209:36640

61.242.114.3:6383

79.112.156.169:10236

95.25.111.173:40781

108.36.82.254:57393

88.8.84.79:56740

118.36.49.220:59561

60.197.149.187:12996

86.26.224.104:39597

120.61.161.250:10023

151.249.239.173:6881

86.178.212.41:28489

95.180.244.144:48245

111.171.83.212:52952

122.164.99.166:1024

201.110.110.63:19314

79.100.52.144:54312

194.219.103.45:24008

178.89.171.19:10003

124.12.192.197:6881

92.96.186.112:31100

207.216.138.62:6881

194.8.234.230:51413

92.220.24.133:6881

2.134.203.233:6881

122.169.237.54:17407

36.232.153.137:16001

130.43.123.202:45689

86.73.45.54:56161

37.215.93.59:27997

78.154.164.176:42780

5.10.134.6:50452

98.176.222.50:61000

64

93.54.90.126:1189

220.81.46.201:51526

39.41.111.173:7702

41.111.41.122:19132

211.108.64.209:20728

178.66.212.41:14865

182.187.103.45:57751

118.41.230.79:52520

186.155.231.45:34294

109.174.113.128:15947

188.6.88.229:16785

99.247.58.79:23197

94.137.237.54:14617

197.203.129.67:10204

5.107.65.67:21618

117.194.114.71:64476

94.153.45.54:32715

2.176.158.50:17404

5.18.178.71:50971

78.130.212.41:63075

86.121.45.54:55858

109.187.1.67:15413

108.199.125.160:38558

83.181.18.121:15859

93.109.242.198:26736

95.86.220.68:27877

37.204.22.24:24146

198.203.28.43:17685

What's particularly interesting, about this campaign, is the fact, that, the Terms of Service (ToS) presented to gullible and socially engineered end users, refers to a well known Web site (**jmobi.net**), directly connected with the market leading [11]**DIY API-enabled mobile malware generating/monetization platform**, extensively profiled in a previously published post.

As cybercriminals continue to achieve a cybercrime-ecosystem wide [12]**standardization**, we'll continue to observe an increase in fraudulent activity, with the cybercriminals behind it, continuing to innovate, on their way to achieve efficient monetization schemes, and risk-forwarding centered fraudulent models, further contributing to the adaptive innovation to be applied to the current [13]**TTPs (tactics, techniques and procedures**) utilized by them.

1. http://www.webroot.com/blog/2013/09/18/affiliate-network-mobile-malware-impersonates-google-play-tricks-users-installing-premium-rate-sms-sending-rogue-apps/

2. http://www.webroot.com/blog/2013/10/08/newly-launched-vds-based-cybercrime-friendly-hosting-provider-helps-facilitate-fraudulentmalicious-online-activity/

3. http://ddanchev.blogspot.com/2013/08/profiling-novel-high-profit-margins.html

4. http://ddanchev.blogspot.com/2013/11/fake-chromefirefoxinternet.html

5. http://ddanchev.blogspot.com/2013/11/a-peek-inside-customer-ized-api-enabled.html

6. http://ddanchev.blogspot.com/2013/09/rogue-iframe-injected-web-sites-lead-to.html

7. http://ddanchev.blogspot.com/2013/08/dissecing-sample-russian-business.html

8. https://www.virustotal.com/en/file/76b2e1a1b7c3079c782e8e1a6238fbf23c93bb3a3cf61a994fd872d478c492d7/analysis/1413910479/

65

9. https://www.virustotal.com/en/file/5ebdf263398fbd4d643c12ea8cb8d1826862ad4b519bda95a09ed004bfc9c6cf/analysis/1413844185/

10. https://www.virustotal.com/en/file/d42aa42fd70f811b0f799f203b6d24ca003ee8cb83ab646de3e0eaa6e968616b/analysis/1413910495/

11. http://ddanchev.blogspot.com/2013/11/a-peek-inside-customer-ized-api-enabled.html

12. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

13. http://www.webroot.com/blog/2013/12/27/cybercrime-trends-2013-year-review/

66

2.

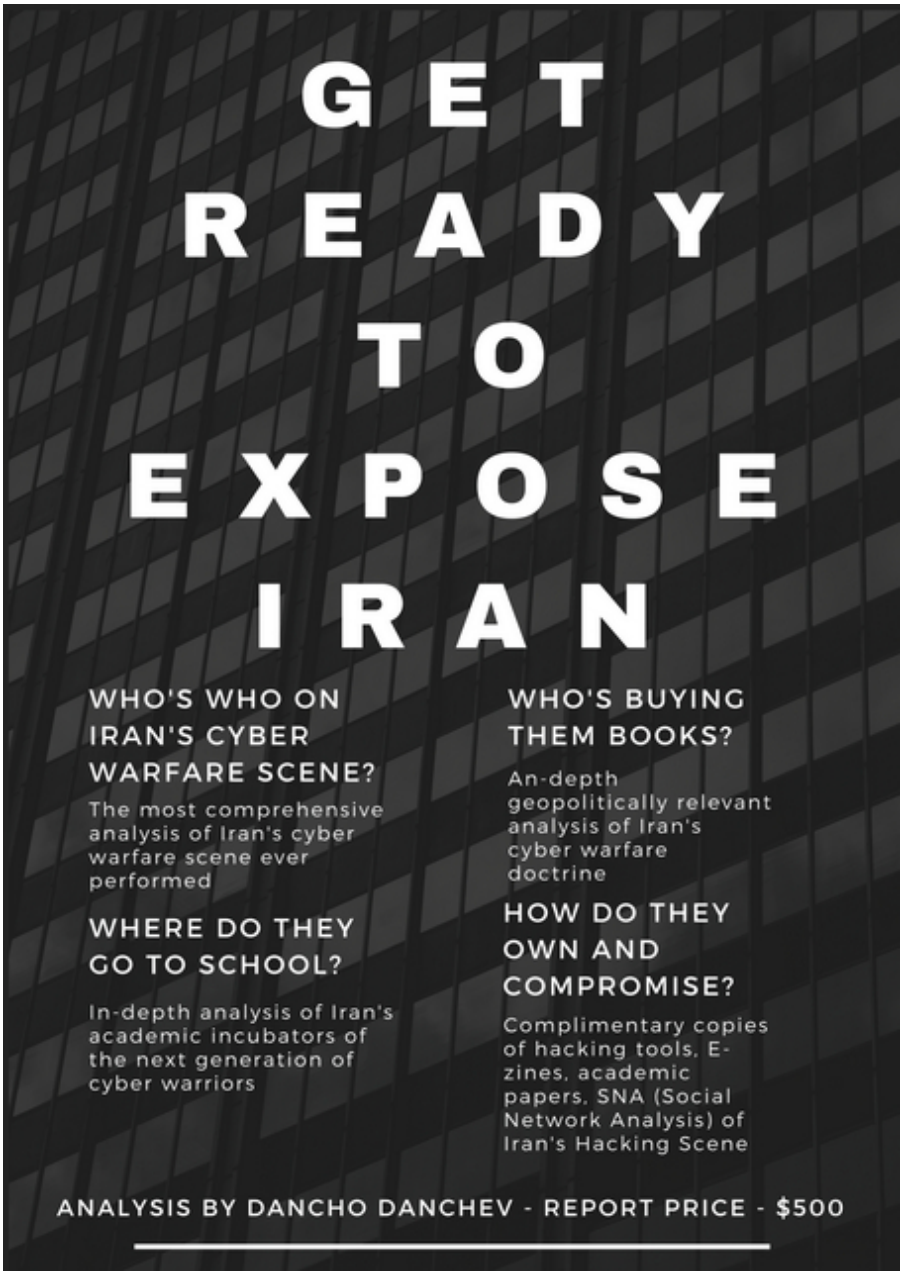
2015

67

2.1

July

68



Assessing The Computer Network Operation (CNO) Capabilities of the Islamic Republic of Iran - Report (2015-07-29 14:45)

Dear blog readers, I would like to let you know, of my latest, publicly released report, on the topic of "[1]**Assessing The Computer Network Operation (CNO) Capabilities of the Islamic Republic of Iran**", a comprehensive, 45 pages, assessment, of Iran’s cyber warfare scene, featuring

exclusive, never-published before, assessments of the country’s cyber warfare doctrine, analysis of the country’s academic incubators of the next generation of cyber warriors, featuring, an exclusive, social network analysis (SNA), of Iran’s hacking scene.

The report, answers the following questions:

• Who’s who on Iran’s Cyber Warfare Scene - the most comprehensive analysis of Iran’s cyber warfare scene, ever performed

69

• Where do they go to school? - in-depth analysis of Iran’s academic incubators of the next generation of cyber warriors

• Who’s buying them books? - in-depth geopolitically relevant analysis of Iran’s cyber warfare doctrine

• How do they own and compromise? - complimentary copies of hacking tools, E-zines, academic papers, SNA (Social Network Analysis) of Iran’s Hacking Scene

An excerpt from the Executive Summary:

" *Today’s growing cyber warfare arms race, prompts for systematic, structured, and multidisciplinary enriched processes to be utilized, in order to anticipate/neutralize and properly attribute an adversary’s strategic, tactical and operational Computer Network Operation (CNO) capabilities, so that an adequate response can be formulated and executed on the basis of a factual research answering some of the most relevant questions in the ’fifth domain’ of warfare - who are our adversaries, what are they up to, when are they going to launch an attack against us, how exactly*

are they going to launch it, and what are they going to target first?

This qualitative analysis (45 pages) seeks to assess the Computer Network Operations (CNO) of Islamic Republic of Iran, through the prism of the adversary's understanding of Tactics, Techniques and Procedures (TTP), a structured and geopolitically relevant, enriched OSINT assessment of their operations, consisting of interpreted hacking literature, videos, and, custom made hacking tools, extensive SNA (Social Network Analysis) of the country's Hacking Ecosystem, real-life personalization of the key individuals behind the groups (personally identifiable photos, personal emails, phone numbers, Blogs, Web Sites, Social Networking accounts etc.). It's purpose is to ultimately empower decision/policy makers, as well as intelligence analysts, with recommendations for countering Islamic Republic of Iran's growing understanding and application of CNO tactics and strategies. "

Request, your, complimentary, copy, of, the, report, by, approaching, me, dancho.danchev@hush.com Enjoy!

1. https://dl.packetstormsecurity.net/papers/general/Iran.rar

70

2.2

August

71

```
127.0.0.1 bobbear.co.uk
127.0.0.1 reed.co.uk
127.0.0.1 seek.com.au
127.0.0.1 scam.com
127.0.0.1 scambusters.org
127.0.0.1 www.guardian.co.uk
127.0.0.1 ddanchev.blogspot.com
127.0.0.1 aic.gov.au
127.0.0.1 google.com.au
127.0.0.1 www.reed.co.uk
```

Historical OSINT: OPSEC-Aware Sprott Asset Management Money Mule Recruiters Recruit, Serve Crimeware, And Malvertisements (2015-08-27 16:02)

Cybercriminals continue multitasking, on their way to take advantage of well proven fraudulent revenue sources, further, positioning themselves as opportunistic market participants, generating fraudulent revenues, [1]**standardizing** and innovating within the context of [2]**OPSEC (Operational Security)** while enjoying a decent market share within the [3]**cybercrime ecosystem**.

In this post, I'll profile a [4]**money mule recruitment campaign**, featuring a custom fake certificate, successfully blocking access to [5]**bobbear.co.uk** as well as my personal blog, further exposing [6]**a malicious infrastructure**, that I'll profile in this post.

Let's assess the campaign, and expose the malicious infrastructure behind it.

The fake Sprott Asset Management sites, entices end users into installing the, the fake, malicious certificate, as a prerequisite, to being working with them, with hosting courtesy of ALFAHOSTNET (AS50793), a well known

cybercrime-friendly malicious hosting provider, known, to have been involved in a variety of malvertising campaigns, including related malicious campaigns, that I'll expose in this post.

Domain name reconnaissance for the malicious hosting provider:

alfa-host.net - (AS50793) - Email:

alitalaghat@gmail.com; Name:

Mohmmad Ali Talaghat (**webalfa.net** -

78.47.156.245 also registered with the same email)

Name Server: NS1.ALFA-HOST.NET

Name Server: NS2.ALFA-HOST.NET

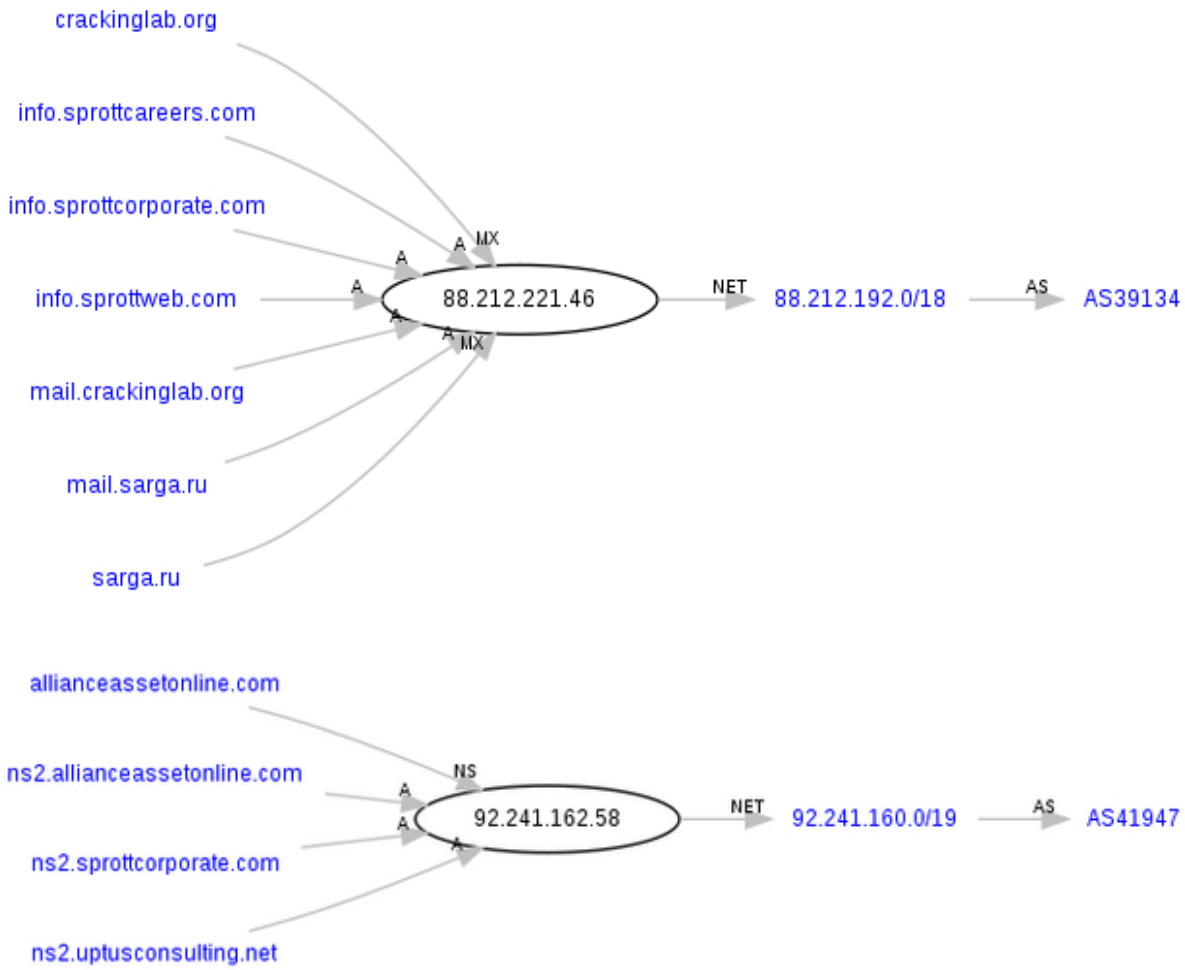
Alfa-host LLP - (AS50793)

person: Romanov Artem Alekseevich

phone: +75.332211183

address: Kazakhstan, Karagandinskaya obl, Karaganda, ul. Erubaeva 57, 14

Upstream provider reconnaissance:



LLC TC "Interzvyazok"

Hvoiki 15/15

04080 Kiev

UKRAINE

phone: +380 44 238 6333

fax: +380 44 238 6333

e-mail: dz (at) intersv (dot) com

The same upstream provider (Interzvyazok; intersv.com) is also known to have offered services to [7]**yet another bulletproof hosting provider in 2011**.

Domain name reconnaissance:

sprottcareers.com - 193.105.207.105; 88.212.221.46

sprottcorporate.com - 193.105.207.105; 88.212.221.46

sprottcorporate.com - 92.241.162.58

sprottweb.com - 193.105.207.105; 88.212.221.46

Domain name reconnaissance:

allianceassetonline.com - 92.241.162.58

allianceassetweb.com - 88.212.221.41

uptusconsulting.net - Email: terrizziboris@googlemail.com - 92.241.162.58

Known to have responded to the same IP (193.105.207.105) are also the following malicious domains:auditthere.ru maccrack.ru

nissanmoto.ru

megatuz.ru

basicasco.ru

megatuz.ru

foreks999.ru

monitod.ru

peeeeee.ru

fra8888.ru

inkognittto.ru

lavandas.ru

Related MD5s known to have phoned back to the same IP (193.105.207.105):MD5: a9442b894c61d13acbac6c59adc67774

MD5:7fd31163fe7d29c61767437b2b1234cd

MD5:d90de03caa80506307fc05a0667246ef

MD5:09241426aac7a4aae12743788ce4cff4

MD5:cb74fb88f36b667e26f41671de8e1841

MD5:8efd31e0f3c251a3c7ef63b377edbf9c

MD5:a750359c72de3fc38d2af2670fd1a343

MD5:f0cbef01f5bd1c075274533f164bb06f

MD5:398b06590179be83306b59cea9da79e5

Related malicious domains known to have been active within (AS50793), ALFAHOSTNET:34real.ru
3pulenepro.net

3weselchak.net

analizes.ru

appppa1.ru

arbuz777.ru

arsenalik.ru

assolo.ru

astramani.ru

basicasco.ru

bits4ever.ru

bonokur.ru

boska7.ru

chudachok9.ru

cosavnos.ru

dermidom44.ru

drtyyyt.ru

dvestekkk.ru

ferdinandi.ru

74

ferzipersoviy.ru

foreks999.ru

fra8888.ru

globus-trio.ru

google-stats.ru

horonili.ru

inkognittto.ru

karlito777.ru

lavandas.ru

ma456.ru

medriop56.ru

megatuz.ru

mnobabla.ru

monitod.ru

offshoreglobal.ru

okrison.com

opitee.ru

otrijek.ru

peeeeee.ru

pohmaroz44.ru

postmetoday.ru

reklamen6.ru

reklamen7.ru

rrrekti.ru

sekretfive.ru

stolimonov.ru

sworo.ru

trio4.ru

update4ever.ru

victorry.ru

vivarino77.ru

vopret.ru

wifipoints.ru

Known to have responded to the same IP (88.212.221.46) in the past, are also the following malicious domains:

liramdelivery.com - Email: carlyle.jeffrey@gmail.com

ffgroupjobs.com - Email: FfGroupJobs@dnsname.info

secretconsumeril.com

Name servers:

ns2.uptusconsulting.net - 92.241.162.58

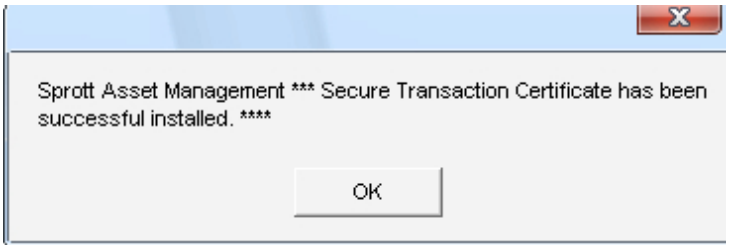
ns2.sprottcorporate.com - 92.241.162.58

ns2.sprottweb.com - 92.241.162.58

allianceassetweb.com - Email: martins.allianceam@gmail.com

Surprise, surprise. We've also got the [8]**following** fraudulent [9]**domains**, responding [10]**to the same** [11]**name server's** IP (**92.241.162.58**; **ns1.oildns.net, ns2.oildns.net**) back in 2009.

75



What's particularly interesting, is the fact, that in 2010, we've also got (92.241.162.58) hosting the following malicious MD5s:

MD5: 8ee5435004ad523f4cbe754b3ecdb86e

MD5: 38f5e6a59716d651915a895c0955e3e6

We've also got ns1.oildns.net responding to (93.174.92.220), with the actual name server, known to have hosted, the following malicious MD5s:

MD5: 5ae4b6235e7ad1bf1e3c173b907def17

Sample detection rate for the malicious certificate:

[12]MD5:

ec39239accb0edb5fb923c25ffc81818 - detected by 23 out of 42 antivirus scanners as Gen:Trojan.Heur.SFC.juZ@aC7UB8eib

Sample detection rate for the HOSTS file modifying sample:

[13]MD5:

969001fcc1d8358415911db90135fa84 - detected by 14 out of 42 antivirus scanners as Trojan.Generic.4284920

Once executed, the sample successfully modifies, the HOSTS file on the affected hosts, to block access to:
127.0.0.1 google.com

127.0.0.1 google.co.uk

127.0.0.1 www.google.com

127.0.0.1 www.google.co.uk

127.0.0.1 suckerswanted.blogspot.com

127.0.0.1 ideceive.blogspot.com

127.0.0.1 www.bobbear.co.uk

127.0.0.1 bobbear.co.uk

127.0.0.1 reed.co.uk

127.0.0.1 seek.com.au

127.0.0.1 scam.com

127.0.0.1 scambusters.org

127.0.0.1 www.guardian.co.uk

127.0.0.1 ddanchev.blogspot.com

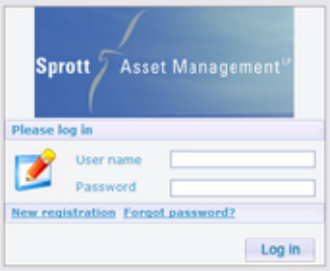
127.0.0.1 aic.gov.au

127.0.0.1 google.com.au

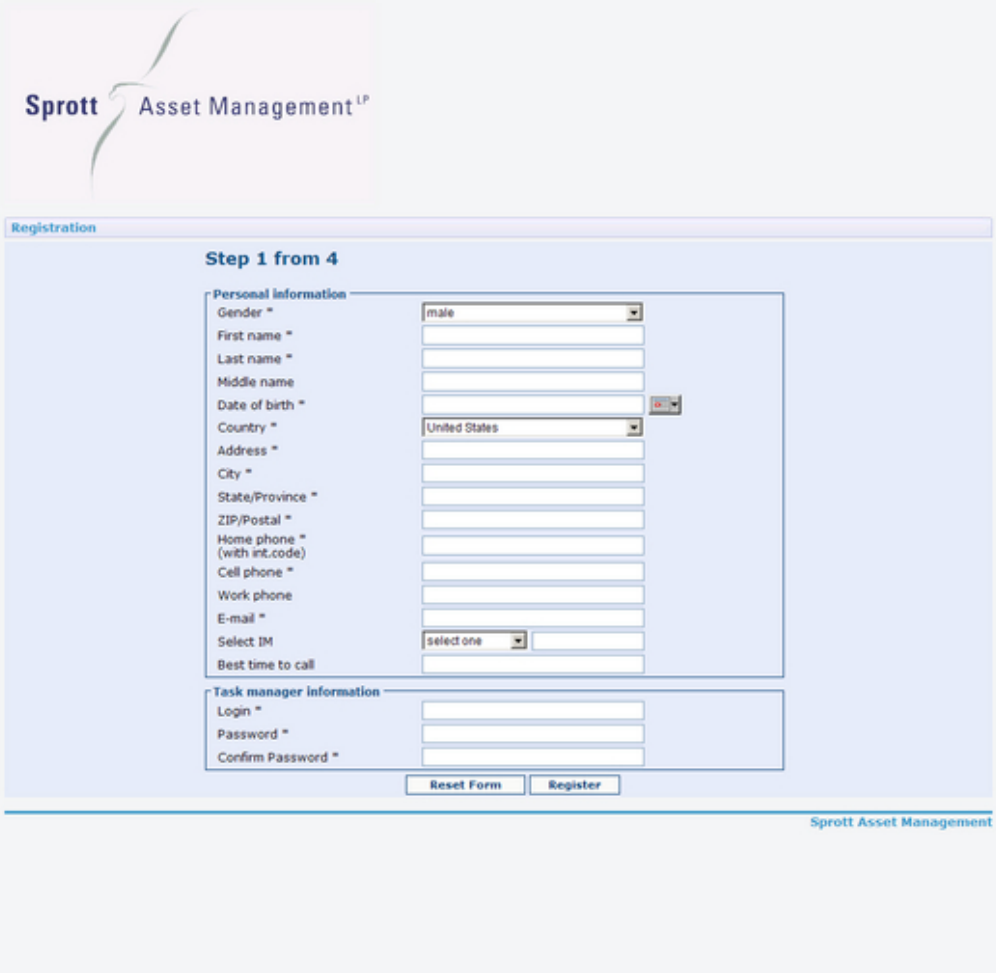
127.0.0.1 www.reed.co.uk

209.171.44.117 www.sprott.com

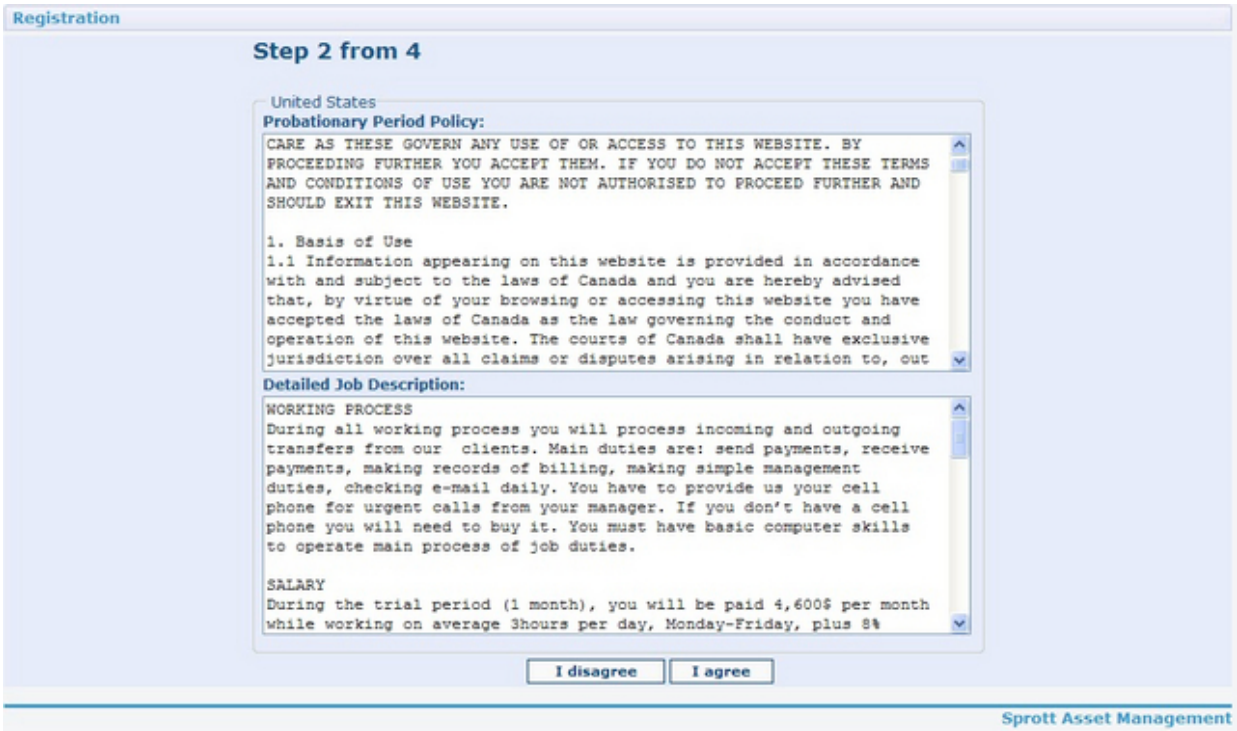
209.171.44.117 sprott.com


Sprott
Asset Management
Please log in
User name
Password
New registration
Forgot password?
Log in

77


Sprott Asset Management LP
Registration
Step 1 from 4
Personal information
Gender *
male
First name *
Last name *
Middle name
Date of birth *
Country *
United States
Address *
City *
State/Province *
ZIP/Postal *
Home phone * (with int.code)
Cell phone *
Work phone
E-mail *
Select IM
select one
Best time to call
Task manager information
Login *
Password *
Confirm Password *
Reset Form
Register
Sprott Asset Management

78



Sample confirmation email courtesy of Sprott Asset Management:

WORKING PROCESS

During all working process you will process incoming and outgoing transfers from our clients. Main duties are: send payments, receive payments, making records of billing, making simple management duties, checking e-mail daily.

You have to provide us your cell phone for urgent calls from your manager. If you don't have a cell phone you will need to buy it. You must have basic computer skills to operate main process of job duties.

SALARY

During the trial period (1 month), you will be paid 4,600 $ per month while working on average 3hours per day, Monday-Friday, plus 8 % commission from every payment received and processed. The salary will be sent in the form of wire transfer directly to your account or you may take it from received funds directly. After the trial period your base pay salary will go up to 6,950 $ per month, plus 10 % commission.

FEES & TRANSFERING PROCEDURE

All fees are covered by the company. The fees for transferring are simply deducted from the payments received.

Customer will not contact you during initial stage of the trial period. After three weeks of the trial period you will begin to have contact with the customers via email in regards to collection of the payments. For the first three weeks you will simply receive all of the transferring details, and payments, along with step by step guidance from your supervisor. You will be forwarding the received payments through

transferring agents such as Western Union, Money Gram, any P2P agents or by wire transferring.

WESTERN UNION & MONEYGRAM

1. As soon as You receive money transfers from our clients you are supposed to cash it in your bank.

2. You will need to pick up the cash physically at the bank, as well as a transfer to MoneyGram.

3. Please use MoneyGram, located not in your bank, because this providing of anonymosty of our clients.

4. The cashed amounts of money should be transferred to our clients via MoneyGram/Western Union.

79

according to our transfer instructions except all the fees. The fees are taken from the amount cashed.

5. Not use online service, only physical presence in an office of bank and Western Union.

6. Just after you have transferred money to our clients, please contact your personal manager via e-mail (confirmation of the transfer)

and let him (her) know all the details of your Western Union transfer: SENDER'S NAME, CONTACT DETAILS, ADRESS, AND A REFERENCE NUMBER,

PLEASE BE VERY CAREFUL WHEN YOU RESEND FUNDS, THERE MUST BE NO MISTAKES, because our client will not be able to withdraw the funds.

7. All procedures have to take 1-2 hours, because we have to provide and verify the safety of our clients‘ money (we have to inform them about all our actions).

Your manager will support you in any step of application process, if you have any questions you may ask it anytime.

Go through related research regarding money mule recruitment:

• [14]Profiling a Novel, High Profit Margins Oriented, Legitimate Companies Brand-Jacking Money Mule Recruitment Scheme

• [15]Spotted: cybercriminals working on new Western Union based ‘money mule management’ script

• [16]Keeping Money Mule Recruiters on a Short Leash - Part Eleven

• [17]Keeping Money Mule Recruiters on a Short Leash - Part Ten

• [18]Keeping Money Mule Recruiters on a Short Leash - Part Nine

• [19]Keeping Money Mule Recruiters on a Short Leash - Part Eight - Historical OSINT

• [20]Keeping Money Mule Recruiters on a Short Leash - Part Seven

• [21]Keeping Money Mule Recruiters on a Short Leash - Part Six

• [22]Keeping Money Mule Recruiters on a Short Leash - Part Five

• [23]The DNS Infrastructure of the Money Mule Recruitment Ecosystem

• [24]Keeping Money Mule Recruiters on a Short Leash - Part Four

• [25]Money Mule Recruitment Campaign Serving Client-Side Exploits

• [26]Keeping Money Mule Recruiters on a Short Leash - Part Three

• [27]Money Mule Recruiters on Yahoo!’s Web Hosting

• [28]Dissecting an Ongoing Money Mule Recruitment Campaign

• [29]Keeping Money Mule Recruiters on a Short Leash - Part Two

• [30]Keeping Reshipping Mule Recruiters on a Short Leash

• [31]Keeping Money Mule Recruiters on a Short Leash

• [32]Standardizing the Money Mule Recruitment Process

80

• [33]Inside a Money Laundering Group’s Spamming Operations

• [34]Money Mule Recruiters use ASProx’s Fast Fluxing Services

• [35]Money Mules Syndicate Actively Recruiting Since 2002

1. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

2. http://www.webroot.com/blog/tag/opsec/

3. http://www.webroot.com/blog/2013/12/27/cybercrime-trends-2013-year-review/

4. http://ddanchev.blogspot.com/2013/08/profiling-novel-high-profit-margins.html

5. http://ddanchev.blogspot.com/2008/11/ddos-attack-against-bobbearcouk.html

6. http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html

7. http://www.abuse.ch/?p=3130

8. http://www.bobbear.co.uk/liram-delivery-service.html

9. http://www.bobbear.co.uk/avicenna.html

10. http://www.bobbear.co.uk/asset-management-company.html

11. http://www.bobbear.co.uk/alliance-asset-management.html

12. https://www.virustotal.com/file/1af2de0503eeb8213284f03e651765fb6003233d6e4ce0eab40676ba9e66123e/analysis/

13. https://www.virustotal.com/file/12f0c720c629a29e5e2aca486370c549d77057259f1dd38aca50c078aaf7ed57/analysis/

14. http://ddanchev.blogspot.com/2013/08/profiling-novel-high-profit-margins.html

15. http://ddanchev.blogspot.com/2013/08/profiling-novel-high-profit-margins.html

16. http://ddanchev.blogspot.com/2011/08/keeping-money-mule-recruiters-on-short.html

17. http://ddanchev.blogspot.com/2011/07/keeping-money-mule-recruiters-on-short.html

18. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_30.html

19. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_25.html

20. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short.html

21. http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html

22. http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html

23. http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html

24. http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html

25. http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html

26. http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html

27. http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html

28. http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html

29. http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html

30. http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html

31. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

32. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

33. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

34. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

35. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

Historical OSINT - How TROYAK-AS Utillized BGP-over-VPN to Serve the Avalance Botnet (2015-08-28 16:15)

Historical OSINT is a crucial part of an intelligence analyst's mindset, further positioning a growing or an emerging trend,

as a critical long term early warning system indicator, highlighting the importance, of current and emerging trends.

In this post, I'll discuss Troyak-AS, a well-known cybercrime-friendly hosting provider, that represented, the growing factor, for the highest percentage of malicious and fraudulent activity online, throughout 2010, its upstream provider NetAssist LLC, and most importantly, a malicious innovation applied by cybercriminals, at the time, namely the introduction of malicious netblocks and ISPs, within the RIPE registry, relying on [1]**OPSEC (Operational Security)** and basic evasive practices.

According to RSA, the [2]**Ukrainian based ISP NetAssist LLC** is listed as a legitimate ISP, one whose services haven't been abused in any particular cybercrime-friendly way.

This analysis, will not only prove, otherwise, namely, that [3]**NetAssist LLC's** involvement in introducing a dozen of

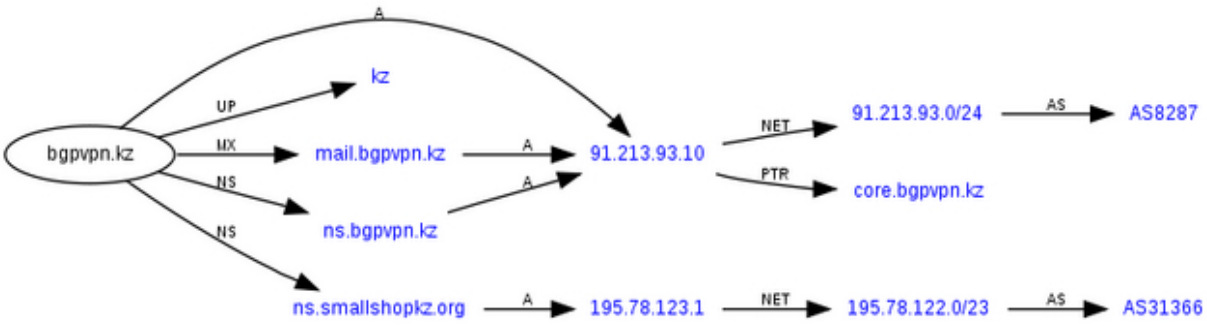
[4]**cybercrime friendly networks** – including [5]**TROYAK-AS** – has been taking place for purely commercial reasons, with the ISP charging thousands of euros for the process, but also, expose a malicious innovation applied on behalf of [6]**opportunistic cybercriminals**, at the time, namely, the introduction of innovative bulletproof hosting tactics, techniques and procedures.

Domain name reconnaissance:

troyak.org - 74.208.21.227 (AS8560); 195.93.184.1 (AS44310) - Email: staruy.rom@troyak.org; staruy.rom@inbox.ru **smallshopkz.org** - 195.78.123.1 (AS12570)

The site is closed for redesign

For support and connection, please call: (095)2734191, e-mail:support@ctlan.net.



Name servers:

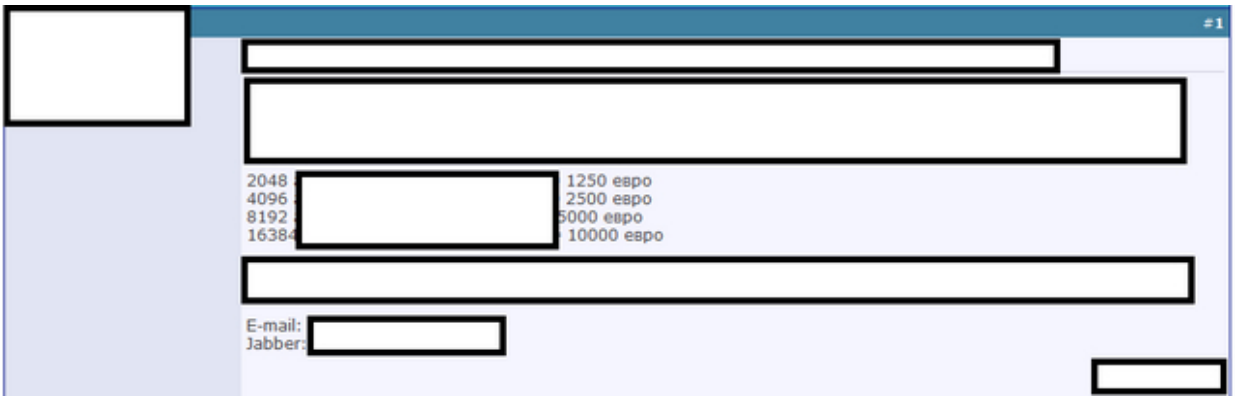
ns.troyak.org - 195.93.184.1 - (AS44307) ALYANSHIMIYA

ns.bgpvpn.kz - 91.213.93.10

ns.smallshopkz.org (195.78.123.1) is also known to have offered DNS services, to **prombd.net** (AS44107) PROMBUD-DETAL (AS50215 Troyak-as at the time responding to **ctlan.net**) - 91.201.30.1, and **vesteh.net** (AS47560) VESTEH-NET

91.200.164.1

83



Domain name reconnaissance:

bgpvpn.kz

Organization Using Domain Name

Name.....: Mykola Tabakov

Organization Name.....: Mykola Tabakov

Street Address.....: office 211, ul. Pushkina, dom 166

City.....: Astana

State.....: Astana

Postal Code.....: 010000

Country.....: KZ

Administrative Contact/Agent

NIC Handle.....: CA537455-RT

Name.....: Mykola Tabakov

Phone Number.....: +7.7022065468

Fax Number.....: +7.7022065468

Email Address.....: tabanet@mail.ru

Nameserver in listed order:

*Primary server.....: **ns.bgpvpn.kz***

*Primary ip address.....: **91.213.93.10***

Domain name reconnaissance:

smallshopz.biz

Domain Name:SMALLSHOPKZ.ORG

Created On:30-Oct-2009 13:42:14 UTC

Last Updated On:19-Mar-2010 14:39:19 UTC

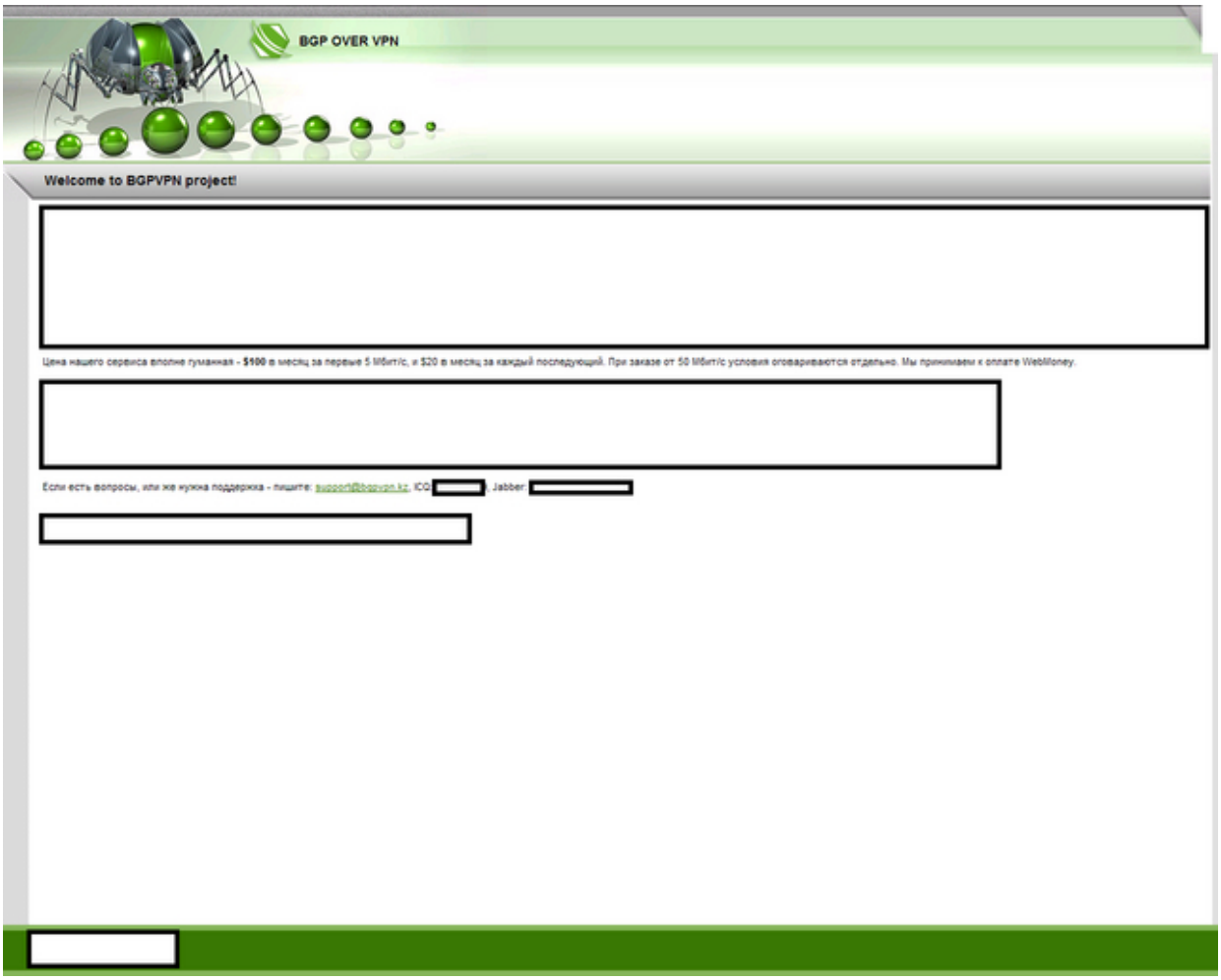
Expiration Date:30-Oct-2010 13:42:14 UTC

Sponsoring Registrar:Directi Internet Solutions Pvt. Ltd. d/b/a PublicDomainRegistry.com (R27-LROR) Status:CLIENT TRANSFER PROHIBITED

Registrant ID:DI _10606443

Registrant Name:Vladimir Vladimirovich Stebluk

Registrant Organization:N/A



Registrant Street1:off. 306, Bulvar Mira, 16

Registrant Street2:

Registrant Street3:

Registrant City:Karaganda

Registrant State/Province:Qaraghandyoblysy

Registrant Postal Code:100008

Registrant Country:KZ

Registrant Phone:+7.7012032605

Registrant Phone Ext.:

Registrant FAX:

Registrant FAX Ext.:

Registrant Email:vladcrazy@smallshopkz.org

NetAssist LLC (netassist.ua) (AS29632) reconnaissance:

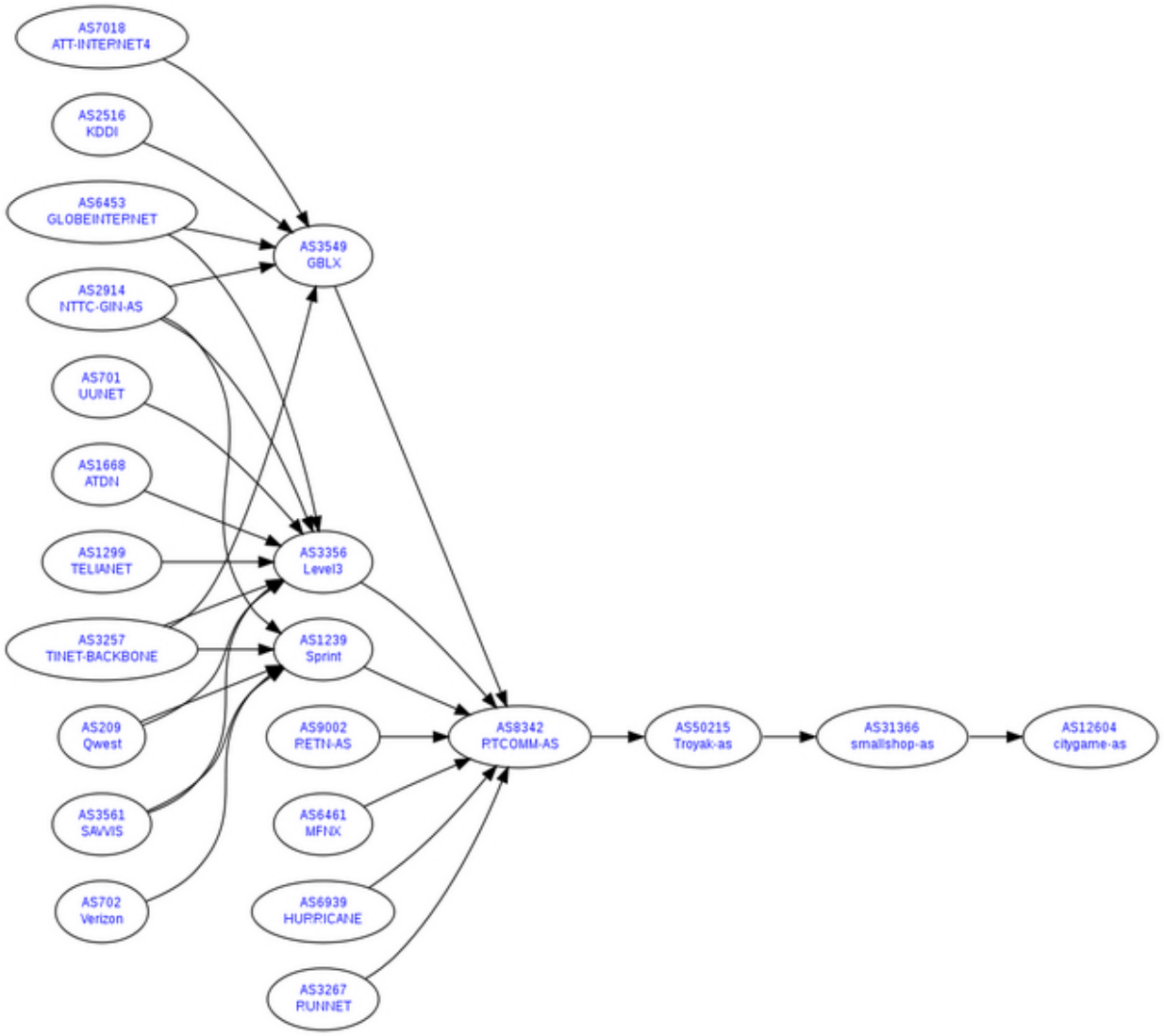
inetnum: 62.205.128.0 - 62.205.159.255

netname: UA-NETASSIST-20080201

descr: NetAssist LLC

country: UA

org: ORG-NL64-RIPE



admin-c: MT6561-RIPE

admin-c: AVI27-RIPE

tech-c: MT6561-RIPE

tech-c: APP18-RIPE

status: ALLOCATED PA

mnt-by: RIPE-NCC-HM-MNT

mnt-lower: MEREZHA-MNT

mnt-routes: MEREZHA-MNT

mnt-domains: MEREZHA-MNT

source: RIPE # Filtered

organisation: ORG-NL64-RIPE

org-name: NetAssist LLC

org-type: LIR

address: NetAssist LLC

86

Max Tulyev

GEROEV STALINGRADA AVE APP 57 BUILD 54

04213 Kiev

UKRAINE

phone: +380 44 5855265

fax-no: +380 44 2721514

e-mail: info@netassist.kiev.ua

admin-c: AT4266-RIPE

admin-c: KS3536-RIPE

admin-c: MT6561-RIPE

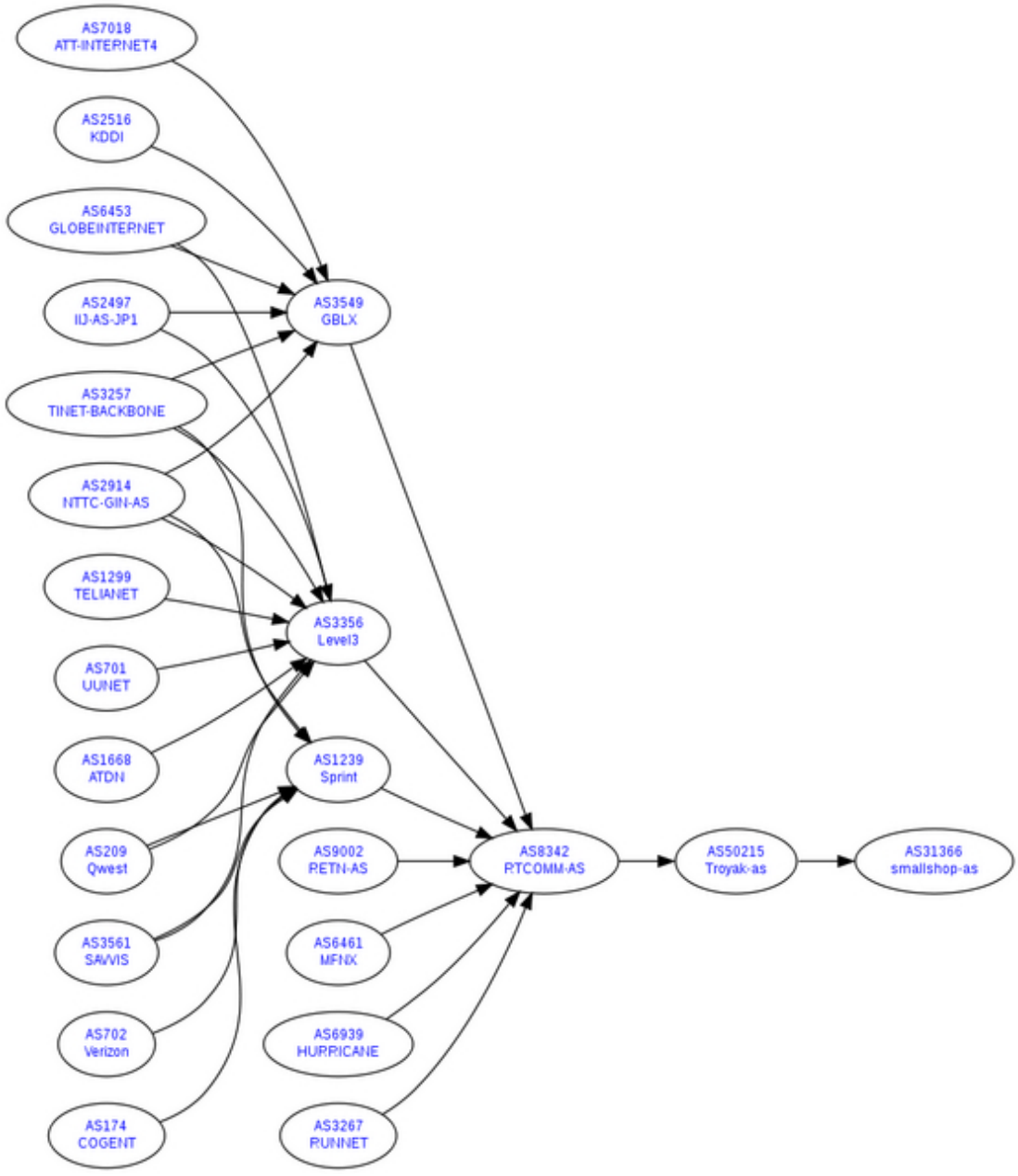
mnt-ref: RIPE-NCC-HM-MNT

mnt-ref: MEREZHA-MNT

mnt-by: RIPE-NCC-HM-MNT

source: RIPE # Filtered

87



person: Max Tulyev

address: off. 32, 12 Artema str.,

address: Kiev, Ukraine

remarks: Office phones

phone: +380 44 2398999

phone: +7 495 7256396

phone: +1 347 3414023

phone: +420 226020344

remarks: GSM mobile phones, SMS supported

phone: +7 916 6929474

phone: +380 50 7775633

remarks: Fax is in auto-answer mode

fax-no: +380 44 2726209

remarks: The phone below is for emergency only

88

remarks: You can also send SMS to this phone

phone: +88216 583 00392

remarks:

remarks: Jabber ID mt6561@jabber.kiev.ua

remarks: SIP 7002@195.214.211.129

e-mail: maxtul@netassist.ua

e-mail: president@ukraine.su

nic-hdl: MT6561-RIPE

mnt-by: MEREZHA-MNT

source: RIPE # Filtered

person: Alexander V Ivanov

address: 14-28 Lazoreviy pr

address: Moscow, Russia

address: 129323

phone: +7 095 7251401

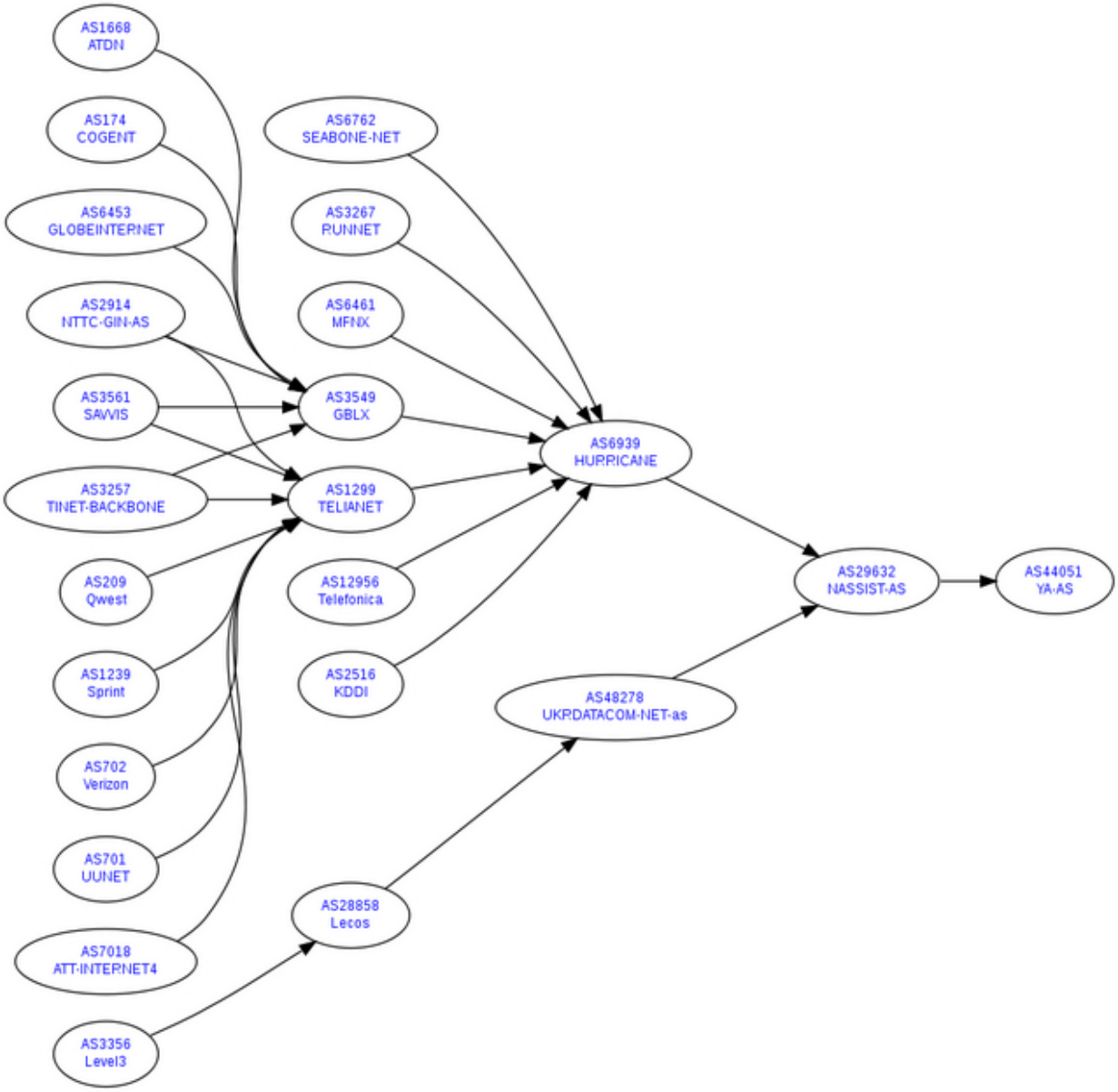
fax-no: +7 095 7251401

e-mail: ivanov077@gmail.com

nic-hdl: AVI27-RIPE

mnt-by: MEREZHA-MNT

source: RIPE # Filtered



person: Alexey P Panyushev

address: 8-142, Panferova street

address: Moscow, Russia

address: 117261

phone: +7 903 6101520

fax-no: +7 903 6101520

e-mail: panyushev@gmail.com

nic-hdl: APP18-RIPE

mnt-by: MEREZHA-MNT

source: RIPE # Filtered

Is NetAssist LLC, on purposely offering its services, for the purpose of orchestrating cybercrime-friendly campaigns, in a typical bulletproof cybercrime friendly fashion, or has it been abused, by an opportunistic cybercriminals, earning fraudulently obtained revenues in the process? Based on the analysis in this post, and the fact, that the company, continues offering IPv4 RIPE announcing services, I believe, that on the majority of occasions, the company 90

has had its services abused, throughout 2010, leading to the rise of the Avalance bothet.

I expect to continue observing such type of abuse, however, in a [7]**cybercrime ecosystem**, dominated, by the abuse of legitimate services, I believe that cybercriminals will continue efficiently bypassing defensive measures in place, through the abuse and compromise of legitimate infrastructure.

This post has been reproduced from [8]Dancho Danchev's blog .

1. http://www.webroot.com/blog/tag/opsec/

2. http://rsa.com/blog/blog_entry.aspx?id=1610

3. https://www.abuse.ch/?p=2417

4. http://ddanchev.blogspot.com/2010/05/avalanche-botnet-and-troyak-as.html

5. http://www.zdnet.com/article/troyak-as-the-cybercrime-friendly-isp-that-just-wont-go-away/

6. http://ddanchev.blogspot.com/2010/03/as50215-troyak-as-taken-offline-zeus-c.html

7. http://www.webroot.com/blog/2013/12/27/cybercrime-trends-2013-year-review/

8. http://ddanchev.blogspot.com/

Document Outline